

UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR



Máster Universitario en Investigación e
Innovación en Inteligencia Computacional y
Sistemas Interactivos

TRABAJO FIN DE MÁSTER

**VERIFICACIÓN DE FIRMA
DINÁMICA: NUEVOS ENFOQUES
BASADOS EN LA ESTABILIDAD DE
MUESTRAS Y TRAZOS**

Autor: Carlos González García

Tutor: Rubén Vera Rodríguez

NOVIEMBRE 2020

VERIFICACIÓN DE FIRMA DINÁMICA: NUEVOS ENFOQUES BASADOS EN LA ESTABILIDAD DE MUESTRAS Y TRAZOS

Autor: Carlos González García
Tutor: Rubén Vera Rodríguez

Biometric and Data Pattern Analytics - BiDA Lab
Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
NOVIEMBRE 2020

Resumen

En este Trabajo de Fin de Máster se realiza un estudio de los sistemas de verificación basados en firma manuscrita dinámica desde un enfoque novedoso: el análisis de la estabilidad de los trazos de la firma genuina de un usuario, con el objetivo de mejorar el rendimiento de los sistemas de verificación actuales.

En primer lugar, se hace un estudio de los sistemas de verificación de firma actuales que, en la gran mayoría de situaciones ya obtienen excelentes resultados. Sin embargo, los sistemas de verificación se enfrentan a dos dificultades: por un lado, las firmas introducidas mediante el dedo, más populares en estos días, no obtienen tan buenos resultados como las firmas introducidas mediante un útil específico de escritura como es un *stylus*. Por otro lado, los sistemas de verificación tienen que deben lidiar con falsificaciones cada vez de mayor calidad: deben ser capaces de identificar falsificaciones realizadas por impostores que tenían a su disposición toda la información relativa a la firma genuina a falsificar, lo que permite hacer a los impostores falsificaciones muy similares a las firmas genuinas de los usuarios.

En segundo lugar, se ha realizado un estudio del impacto de la detección y utilización de los trazos y muestras más estables de una firma sobre el rendimiento de los sistemas actuales. Con los resultados obtenidos, se han estudiado y propuesto otras posibles métricas que puedan dar indicios de potenciales falsificaciones, como por ejemplo, el número de trazos en los que se divide una firma en base a su perfil de velocidad.

Por último, una vez analizados los resultados obtenidos y extraídas las conclusiones al respecto, se ha propuesto una serie de líneas de investigación para trabajos futuros.

Palabras Clave

Sistema de verificación biométrico, firma manuscrita, estabilidad de trazos, perfil de velocidad, DTW.

Abstract

In this Master's Thesis, a study of verification systems based on dynamic handwritten signature is carried out from a novel approach: the analysis of the stability of the strokes of a user's genuine signature, with the aim of improving the performance of current verification systems.

Firstly, a study of the current signature verification systems has been carried out. In the majority of situations, these systems already obtain excellent results. However, verification systems face two difficulties: on the one hand, the signatures entered using the finger, more popular these days, do not obtain as good results as the signatures entered using a specific writing tool such as a stylus pen. On the other hand, verification systems have to deal with increasingly higher quality forgeries: they must be able to identify forgeries made by imposters who had at their disposal all the information related to the genuine signature to forge, which allows them to do forgeries very similar to genuine user signatures.

Secondly, a study has been carried out on the impact of detecting and using the most stable strokes and samples of a signature on the performance of current verification systems. With the results obtained, other possible metrics, which could give indications of potential forgeries, have been studied and proposed, such as the number of strokes into which a signature is divided based on its velocity profile.

Finally, once the results obtained have been analyzed and the conclusions drawn in this regard, several lines of research have been proposed for future work.

Key words

Biometric verification system, handwritten signature, stability of strokes, velocity profile, DTW.

Agradecimientos

En primer lugar, me gustaría dar las gracias a mi tutor Rubén Vera por haberme dado la oportunidad de hacer este Trabajo de Fin de Máster. Desde el día que nos conocimos (hace ya más de 2 años), ha estado dispuesto a ayudarme en todo lo que ha sido necesario y ha estado atento a cualquier duda o sugerencia que yo pudiese tener.

Agradecer también a mi familia por su apoyo constante y por haber sido una fuente de motivación continua durante todos los años que llevo pisando este mundo.

Por último me gustaría agradecer a mis compañeros de informática, de teleco y del máster, y a mis amigos de Colmenar Viejo (mejor dicho, *de colme*) por haber conseguido que vea la universidad como mi segunda casa y por todos esos momentos divertidos que hemos compartido.

Carlos González García
Noviembre 2020

Índice general

Índice de Figuras	IX
Índice de Tablas	XI
1. Introducción	1
1.1. Motivación del proyecto	1
1.2. Objetivos	2
1.3. Metodología y plan de trabajo	3
1.4. Organización de la memoria	3
2. Estado del arte	5
2.1. La biometría en la actualidad	5
2.2. Los rasgos biométricos: la firma manuscrita	5
2.2.1. Tipos de sistemas biométricos basados en firma manuscrita	7
2.3. Sistemas de verificación de firma manuscrita	8
2.3.1. Sistemas de verificación de firma dinámica en función de las características de las firmas que utilizan	8
2.3.2. Tipos de falsificaciones	8
2.4. Sistema de verificación de firma manuscrita dinámica basado en <i>local features</i>	9
2.4.1. <i>Dynamic Time Warping</i> (DTW)	11
2.4.2. Funcionamiento de un sistema de verificación de firma manuscrita basado en <i>local features</i>	12
2.5. Más allá de DTW: Técnicas basadas en <i>deep learning</i>	13
3. Bases de datos de firma manuscrita.	17
3.1. Bases de datos de firma manuscrita	17
3.2. La base de datos <i>DeepSignDB</i>	17
3.2.1. <i>e-BioSign</i> DS1	18
3.2.2. <i>e-BioSign</i> DS2	19
3.3. La base de datos <i>MobileTouchDB</i>	20
3.3.1. Introducción y contexto	20
3.3.2. Pre-procesado de la base de datos	21

3.4. Generación de falsificaciones para <i>MobileTouchDB</i>	21
3.4.1. Protocolo de generación de las falsificaciones	22
3.4.2. Generación de las <i>skilled forgeries</i> estáticas	22
3.4.3. Generación de las <i>skilled forgeries</i> dinámicas	23
3.4.4. Pre-procesado de las falsificaciones generadas y eliminación de usuarios repetidos	24
4. Método Propuesto	27
4.1. Sistema propuesto	27
4.2. Segmentación de una firma en trazos mediante su perfil de velocidad	28
4.2.1. Emparejamiento de trazos entre firmas genuinas	30
4.2.2. Identificación de los trazos más estables de las firmas genuinas de un determinado usuario	31
4.2.3. Identificación de las muestras más estables de las firmas genuinas de un determinado usuario	33
4.2.4. Relaciones entre las muestras y trazos más estables de una firma	34
4.3. Métodos alternativos: extracción de trazos mediante el modelo Sigma-Lognormal	35
4.3.1. División de una firma en <i>lognormal strokes</i>	35
4.3.2. Cálculo de la distancia entre dos firmas en base a sus <i>lognormal strokes</i>	37
4.3.3. Explotación de los <i>lognormal strokes</i> para mejorar el rendimiento de los sistemas de verificación de firma manuscrita	37
5. Experimentos.	39
5.1. Introducción	39
5.2. Bases de datos	39
5.3. Estabilidad de trazos como herramienta para la detección de falsificaciones	41
5.3.1. Protocolo experimental	41
5.3.2. Sistema de referencia	42
5.3.3. Resultados	42
5.4. Estabilidad de trazos entre firmas introducidas mediante <i>stylus</i> y dedo	50
5.4.1. Protocolo experimental	50
5.4.2. Resultados	50
5.5. Evaluación de las falsificaciones generadas para la base de datos <i>MobileTouchDB</i> y estudio del impacto de los trazos más estables en la etapa de verificación	54
6. Conclusiones y trabajo futuro	57
6.1. Conclusiones	57
6.2. Trabajo futuro	58
Bibliografía	59

Índice de Figuras

2.1. Arquitectura del sistema de verificación de firma manuscrita basado en <i>Time-Aligned Recurrent Neural Networks</i> (TA-RNNs).	14
3.1. Ejemplo de tableta digitalizadora Wacom y bolígrafo <i>stylus</i>	18
3.2. Ejemplos de las dinámicas de firmado (evolución de una firma en el tiempo) de una determinada firma de ejemplo.	23
3.3. Ejemplo de una firma genuina de la base de datos <i>MobileTouchDB</i> (imagen izquierda) y una <i>skilled forgery</i> estática de ejemplo.	24
3.4. Ejemplo de una firma genuina de la base de datos <i>MobileTouchDB</i> (imagen izquierda) y una <i>skilled forgery</i> dinámica de ejemplo.	24
4.1. División del espacio de velocidades para generar trazos grandes (imagen superior), trazos medianos (imagen central) y trazos pequeños (imagen inferior). Los puntos negros indican los cambios de trazos.	29
4.2. Ejemplo de firma manuscrita (imagen izquierda) y su descomposición en trazos mediante el perfil de velocidad (imagen derecha).	30
4.3. Ejemplo de la descomposición en trazos según el perfil de velocidad de dos versiones de la firma genuina de un determinado usuario.	31
4.4. En rojo se marcan los trazos más estables de la firma de un usuario, representados sobre 4 de sus firmas genuinas. La imagen superior izquierda representa la firma <i>template</i>	32
4.5. <i>Direct Matching Points</i> extraídos mediante DTW entre dos firmas genuinas de un usuario de la base de datos <i>eBioSign DS1</i>	33
4.6. Selección de DMPs más estables de 4 firmas genuinas de un usuario de la base de datos <i>eBioSign DS1</i>	34
4.7. En las imágenes superiores se muestran los trazos y muestras más estables de la firma de un usuario de la base de datos <i>eBioSign DS1</i>	35
4.8. Tiempos característicos de una <i>lognormal</i>	37
5.1. Ejemplos de dos firmas genuinas de la base de datos <i>e-BioSign</i>	40

5.2. División en intervalos del EER obtenido. Las barras azules representan el EER promedio de cada intervalo (EERs que van de 0 % a 12 %, EERs que van de 12 % a 24 %, EERs que van de 24 % a 36 %, EERs que van de 36 % a 48 % y EERs que van de 48 % a 100 %) obtenido por el sistema que no tiene en cuenta los trazos estables. Las barras rojas representan el EER promedio obtenido por el sistema que sí tiene en cuenta los trazos estables, para los usuarios que obtuvieron un EER dentro del intervalo de la barra azul de su izquierda cuando se calcularon las comparaciones DTW sin tener en cuenta los trazos estables.	44
5.3. División en intervalos del EER obtenido. Las barras azules representan el EER promedio de cada intervalo (EERs que van de 0 % a 5 %, EERs que van de 5 % a 10 %, EERs que van de 10 % a 15 %, EERs que van de 15 % a 20 % y EERs que van de 20 % a 25 %) obtenido por el sistema que no tiene en cuenta los trazos estables. Las barras rojas representan el EER promedio obtenido por el sistema que sí tiene en cuenta los trazos estables, para los usuarios que obtuvieron un EER dentro del intervalo de la barra azul de su izquierda cuando se calcularon las comparaciones DTW sin tener en cuenta los trazos estables.	46
5.4. Evolución de los <i>scores</i> en función del tamaño de los trazos utilizados en las comparaciones para 3 usuarios diferentes (cada gráfica corresponde con un usuario distinto).	47
5.5. Promedio del número de trazos en los que se divide una firma genuina (de cada color, la barra izquierda) y una falsificación (de cada color, la barra derecha). El color rojo representa la división de la firma en trazos grandes, el azul, en trazos medianos y el verde, en trazos pequeños.	48
5.6. Ejemplos de 2 firmas de diferente complejidad de la base de datos <i>e-BioSign DS2</i> : baja complejidad (imagen izquierda) y alta complejidad (imagen derecha).	49
5.7. Evolución de los <i>scores</i> en diferentes comparaciones. A la izquierda se muestra la evolución para las comparaciones realizadas con la firma de baja complejidad de la figura 5.6 y a la derecha se muestra la evolución para las comparaciones realizadas con la firma de alta complejidad.	50
5.8. Ejemplos de una firma genuina introducida mediante <i>stylus</i> (imagen izquierda) y mediante dedo (imagen derecha) de un determinado usuario de la base de datos <i>e-BioSign DS2</i>	51
5.9. Evolución promedio de los <i>scores</i> en comparaciones genuinas, impostoras y aleatorias en usuarios con firmas introducidas mediante el dedo.	52
5.10. Número promedio de trazos en los que se divide las firmas introducidas mediante el dedo (barras rojas) y mediante <i>stylus</i> (barras azules) de un grupo de usuarios. De cada color, la barra izquierda representa las firmas genuinas del usuario y la barra derecha representa sus falsificaciones.	53
5.11. División en intervalos del EER obtenido. Las barras azules representan el EER promedio de cada intervalo (EERs que van de 0 % a 6 %, EERs que van de 6 % a 12 %, EERs que van de 12 % a 18 %, EERs que van de 18 % a 24 % y EERs que van de 24 % a 30 %) obtenido por el sistema que no tiene en cuenta los trazos estables. Las barras rojas representan el EER promedio obtenido por el sistema que sí tiene en cuenta los trazos estables, para los usuarios que obtuvieron un EER dentro del intervalo de la barra azul de su izquierda cuando se calcularon las comparaciones DTW sin tener en cuenta los trazos estables.	55

Índice de Tablas

2.1. Tipos de rasgos biométricos.	6
2.2. Conjunto de <i>local features</i> utilizado en el presente proyecto. El punto situado sobre alguna de las características (e.g. \dot{x}_n), indica derivada en el tiempo. Tabla adaptada de [1].	10
2.3. Comparativa del rendimiento (EER) ofrecido por un enfoque tradicional de verificación y un nuevo enfoque basado en <i>deep learning</i> . Los términos <i>Skilled</i> y <i>Random</i> hacen referencia respectivamente a los tipos de falsificaciones <i>skilled</i> y <i>random forgeries</i>	14
2.4. Comparativa del rendimiento (EER) ofrecido por dos enfoques de verificación basados en <i>deep learning</i> y un nuevo enfoque basado en <i>deep learning</i> . Los términos <i>Skilled</i> y <i>Random</i> hacen referencia respectivamente a los tipos de falsificaciones <i>skilled</i> y <i>random forgeries</i>	15
3.1. Resumen con las principales características de los 2 <i>datasets</i> de la base de datos <i>e-BioSign</i>	20
4.1. Distribución de las muestras más estables dentro de los diferentes trazos de una firma.	34
4.2. Conjunto de <i>stroke features</i> . Tabla adaptada de [2].	36
5.1. Detalles de la composición de la base de datos que se ha utilizado para realizar los experimentos descritos en el presente capítulo.	40
5.2. Rendimiento en términos de EER obtenido por el sistema de verificación que no utiliza los trazos más estables de la firma y por el sistema de verificación que sí utiliza los trazos más estables de la firma.	43
5.3. Rendimiento en términos de EER obtenido por el sistema de verificación que no utiliza los trazos más estables de la firma y por el sistema de verificación que sí utiliza los trazos más estables de la firma.	45
5.4. Reducción media de los <i>scores</i> en comparaciones genuinas, impostoras y aleatorias, para el caso de firmas introducidas mediante <i>stylus</i> y mediante el dedo. . . .	51
5.5. Rendimiento en términos de EER obtenido por el sistema de verificación que no utiliza los trazos más estables de la firma y por el sistema de verificación que sí utiliza los trazos más estables de la firma. Este proceso de verificación se realizó en la base de datos <i>MobileTouchDB</i>	54

1

Introducción

1.1. Motivación del proyecto

Con la evolución de la informática y los avances tecnológicos, cada vez se hace más necesario el desarrollo de un nuevo paradigma de seguridad que deje de estar centrado en lo que el usuario conoce (contraseñas, pines, etc.) o posee (tarjetas, tokens, etc.) y busque enfocarse en lo que el usuario es (sus rasgos físicos y conductuales). La biometría es la disciplina que estudia los rasgos de los usuarios para su posterior utilización dentro de un sistema informático.

Cuando hablamos de un sistema de verificación hablamos de un sistema que busca determinar si un usuario es quien dice ser o es un impostor. Para realizar esta tarea, los sistemas de verificación se basan en los rasgos fisiológicos y conductuales del usuario. Un ejemplo de verificación biométrica cotidiano es el desbloqueo de nuestro *smartphone* a través de nuestra huella dactilar o a través de nuestros rasgos faciales.

Aunque pueden considerarse muchos rasgos biométricos, uno cuyo estudio es especialmente interesante es la firma manuscrita. La firma manuscrita ha estado ligada a la humanidad desde la Antigüedad: siempre se ha utilizado para probar la identidad del autor de un determinado documento (por ejemplo, un contrato). La utilización de la firma manuscrita para añadir un revestimiento de seguridad adicional a los sistemas informáticos actuales es interesante gracias a las características de la propia firma, que permite desarrollar sistemas de verificación con un rendimiento muy alto, y gracias a que goza de una alta aceptación dentro de la sociedad (un usuario no considerará incómodo tener que introducir su firma en un sensor biométrico).

Los sistemas de verificación biométrica han sido ampliamente estudiados a lo largo de los últimos años, sin embargo, aún cuentan con una serie de retos y complicaciones por delante.

El principal reto al que se enfrentan los sistemas de verificación de firma manuscrita es adaptarse a los nuevos escenarios móviles: tradicionalmente estos sistemas se han implementado mediante el uso de dispositivos específicos, como las tabletas digitalizadoras Wacom, en escenarios controlados, como una oficina bancaria. Sin embargo, otra de las revoluciones que han traído los últimos años es la rápida popularización de dispositivos móviles tipo *smartphone*, lo que abre un mundo de posibilidades para los sistemas de verificación basados en firma manuscrita. Las firmas introducidas mediante el dedo sobre la pantalla de un *smartphone* presentan diferencias notables con respecto a las firmas introducidas mediante un bolígrafo tipo *stylus* sobre la pantalla de una tableta Wacom.

El desarrollo de este Trabajo de Fin de Máster está motivado por los dos siguientes aspectos:

Por un lado, el estudio de un nuevo enfoque que permita mejorar el rendimiento de los sistemas de verificación de firma manuscrita mediante la utilización de la estabilidad de los trazos de una firma. El estudio de los trazos de una firma ha sido ampliamente estudiado en el estado del arte, sin embargo, no existen demasiadas publicaciones que hayan estudiado los trazos más estables de la firma, trazos que permitan caracterizar mejor la firma genuina de un usuario y ayuden a discernir esta de potenciales falsificaciones realizadas por un impostor.

Por otro lado, uno de los principales inconvenientes a los que se está enfrentando el desarrollo de un sistema de verificación basado en firma manuscrita es que no existen grandes bases de datos de firmas introducidas mediante el dedo que permitan entrenar sistemas que obtengan rendimientos similares a los obtenidos en sistemas de verificación basados en firmas introducidas mediante *stylus*. En este Trabajo de Fin de Máster se ha buscado dar un paso más para mejorar las bases de datos de firmas introducidas mediante el dedo existentes, mediante la generación de falsificaciones para una de las bases de datos con más usuarios genuinos [3].

1.2. Objetivos

El desarrollo de este Trabajo de Fin de Máster se ha basado en la consecución de los siguientes objetivos:

1. Mejora del rendimiento de los sistemas de verificación de firma manuscrita basados en firmas introducidas mediante *stylus* y mediante el dedo mediante la detección y utilización de los trazos más estables de la firma genuina de un determinado usuario.
2. Desarrollo de nuevas técnicas, basadas en la estabilidad de muestras y trazos, que detecten indicios de posibles falsificaciones dentro del sistema.
3. Desarrollo de un conjunto de falsificaciones para los usuarios de una de las bases de datos de firmas introducidas mediante el dedo más grandes del estado del arte, para que posteriormente puedan ser utilizadas para la mejora de los sistemas de verificación basados en firmas introducidas mediante el dedo.

Para la consecución de los anteriores objetivos, se han identificado los siguientes pasos a llevar a cabo:

- Estudio del estado del arte de los sistemas de verificación biométrica basados en firma manuscrita, tanto los basados en firmas introducidas mediante un bolígrafo *stylus* como los basados en firmas introducidas mediante el dedo.
- Estudio del estado del arte de las principales técnicas de división de una firma en trazos, para la posterior identificación de los trazos más estables.
- Estudio del estado del arte de los principales algoritmos y técnicas de alineamiento temporal dinámico entre secuencias temporales (en este caso, firmas manuscritas).
- Comprensión del código y programas existentes para la implementación de los sistemas de verificación de firma manuscrita.
- Desarrollo del código y algoritmos necesarios para la división de una firma en sus trazos.
- Desarrollo del código necesario para la detección de los trazos más estables de la firma genuina de un usuario.

- Evaluación exhaustiva del rendimiento de un sistema de verificación que tiene en cuenta la estabilidad de los trazos.
- Estudio de los trazos más estables de las firmas de los usuarios de las principales bases de datos y de sus falsificaciones, para el desarrollo de nuevas métricas que permitan mejorar la detección de potenciales falsificaciones.
- Realización de falsificaciones, de diferentes niveles de complejidad, para las firmas de la base de datos presentada en [3].

1.3. Metodología y plan de trabajo

Con el fin de alcanzar los objetivos citados en la anterior sección, se ha definido la siguiente metodología para el presente Trabajo de Fin de Máster:

- **Estudio del estado del arte:** antes de empezar con el proyecto, es de vital importancia realizar una fase de estudio que permita conocer los principales estudios y avances que se han desarrollado sobre los mismos temas que aborda este trabajo, para adquirir los conocimientos e información necesarios para completar este proyecto de forma exitosa. En concreto, en este trabajo se ha realizado fundamentalmente un estudio de los sistemas de verificación de firma manuscrita existentes y de los principales métodos y algoritmos para la división de una firma en trazos.
- **Estudio del software existente:** antes de poder mejorar el rendimiento ofrecido por un sistema de verificación es necesario un estudio detallado del código utilizado. En concreto, el código a estudiar es el utilizado en el grupo de investigación *Biometrics and Data Pattern Analytics* (BiDA-Lab) de la Universidad Autónoma de Madrid.
- **Desarrollo de software y experimentos:** una vez finalizada la fase de estudio, se ha desarrollado código que permita la detección de los trazos más estables de una firma, para su posterior utilización en los sistemas de verificación basados en firma manuscrita.
- **Evaluación de los resultados obtenidos:** los resultados obtenidos con el sistema propuesto se han comparado con los resultados obtenidos por los sistemas existentes, lo que pone de manifiesto la mejora de rendimiento obtenida.
- **Escritura de la memoria:** una vez completados el estudio y los experimentos llevados a cabo, se ha procedido a describirlos de forma detallada en la presente memoria, siguiendo la estructura comentada en la siguiente sección.

1.4. Organización de la memoria

La presente memoria consta de los siguientes capítulos:

- **Capítulo 1: Introducción.** En este capítulo se detalla la motivación que fundamenta este proyecto, los objetivos a conseguir y la metodología de trabajo seguida.
- **Capítulo 2: Estado del arte.** En este capítulo se realiza un estudio completo de los sistemas de verificación de firma manuscrita.

- **Capítulo 3: Bases de datos de firma manuscrita.** En este capítulo se describen las principales bases de datos de firma manuscrita utilizadas en este proyecto, así como el protocolo de generación de falsificaciones para la base de datos *MobileTouchDB*.
- **Capítulo 4: Método Propuesto.** En este tercer capítulo se describe y comenta el sistema propuesto, basado en detección de trazos estables, para la mejora del rendimiento de los sistemas de verificación actuales.
- **Capítulo 5: Experimentos.** En este capítulo se describen de forma detallada los experimentos realizados para probar que se produce una mejora en el rendimiento de los sistemas de verificación gracias a la utilización de los trazos más estables de la firma de un usuario.
- **Capítulo 6: Conclusión y trabajo futuro.** Por último, en este capítulo se incluyen unas conclusiones para este Trabajo de Fin de Máster y se propone una serie de líneas de investigación para un trabajo futuro.

2

Estado del arte

En este capítulo se describe en detalle el sistema de verificación de firma manuscrita dinámica que se ha utilizado en este Trabajo de Fin de Máster. Adicionalmente, se describen de forma detallada las bases de datos que se han utilizado en este trabajo.

2.1. La biometría en la actualidad

Se conoce como **biometría** a la disciplina basada en el estudio de los rasgos propios, distinguibles e intrínsecos de los seres humanos, y que permiten identificar inequívocamente a un individuo de entre todos los demás.

Con el paso de los años, la biometría ha ganado importancia dentro de los sistemas informáticos, gracias a que permite aumentar significativamente la seguridad de los sistemas actuales, respetando la comodidad y facilidad de uso que perciben los usuarios. Algunos de los principales ejemplos de la implantación de sistemas biométricos en la actualidad son el desbloqueo de los dispositivos móviles mediante huella dactilar o rasgos faciales y el control de acceso a eventos de gran afluencia.

La principal ventaja del uso de técnicas biométricas en sistemas informáticos pasa por el hecho de que permiten añadir un recubrimiento de seguridad adicional a cualquier sistema, sin ser necesario que el usuario tenga que recordar una contraseña u otra información adicional. Este hecho facilita significativamente la implantación y la utilización de las técnicas biométricas. Entre los inconvenientes de la biometría, cabe destacar que hay individuos que, debido a diferentes discapacidades, no poseen determinados rasgos biométricos que permitan su identificación, lo que hace que algunos sistemas biométricos no puedan ser totalmente universales.

2.2. Los rasgos biométricos: la firma manuscrita

Como se ha comentado anteriormente, la biometría se basa en el estudio y la utilización de los rasgos físicos y conductuales de los seres humanos. Los rasgos biométricos más comunes se incluyen en la tabla 2.1. Todo el presente Trabajo de Fin de Máster ha sido desarrollado utilizando como rasgo biométrico la firma manuscrita.

Tipos de rasgos biométricos	
Físicos	Conductuales
Rostro	Escritura
Geometría de la mano	Modo de andar
Iris	Gestos
Venas de retina	Firma manuscrita
Voz	Voz

Tabla 2.1: Tipos de rasgos biométricos.

Otra de las principales ventajas de la biometría como mecanismo para aumentar la seguridad de un sistema informático pasa por el hecho de que los rasgos biométricos son intrínsecos a los individuos y que, que estos sean perdidos, olvidados o modificados maliciosamente es muy poco probable.

Los principales requisitos que deben cumplir los rasgos biométricos para que estos puedan ser incorporados a un sistema informático son los siguientes:

- **Universabilidad:** todos los individuos deben poseer este rasgo biométrico.
- **Distintividad:** dos individuos cualesquiera deben ser suficientemente diferentes desde el punto de vista del rasgo biométrico.
- **Permanencia:** el rasgo biométrico en cuestión no debe sufrir modificaciones con el paso del tiempo.
- **Mensurabilidad:** el rasgo biométrico debe ser cuantificable y medible sin una excesiva dificultad.

Los cuatro requisitos anteriores son considerados como los requisitos fundamentales que debe cumplir todo rasgo biométrico, sin embargo, para que un rasgo biométrico sea considerado apto para su utilización dentro de un sistema informático, es necesario que también cumpla las siguientes tres características:

- El rasgo biométrico en cuestión debe presentar buen **rendimiento** tanto en la fase de captura de los datos por medio de un sensor, como en la fase de utilización del rasgo en un sistema.
- El rasgo biométrico debe gozar de una cierta **aceptabilidad** entre la población, es decir, la sociedad debe sentirse cómoda con su uso.
- El rasgo biométrico debe ser **robusto** frente a intentos de falsificación.

Aunque cumplan todos los requisitos anteriores, todos los rasgos biométricos cuentan con una serie de ventajas e inconvenientes. En concreto, entre las ventajas de la **firma manuscrita** destaca su facilidad de cuantificación y mensurabilidad (es decir, es fácil capturarla mediante un sensor) y su amplia aceptación dentro de la sociedad (como se ha comentado en la introducción de esta memoria, desde la Antigüedad, la humanidad ha utilizado la firma como medio para probar la identidad del autor de un determinado documento, como por ejemplo, contratos o préstamos).

En cuanto a los inconvenientes que presenta la firma manuscrita como rasgo biométrico, cabría destacar los siguientes:

- **Alta variabilidad *intra-clase***: es habitual encontrar diferencias entre distintas versiones de la firma de un individuo, todas ellas versiones genuinas, pero que introducen variabilidades en el sistema, que es necesario tener en cuenta a la hora de verificar la identidad de una persona.
- **Baja variabilidad *inter-clase***: los sistemas de verificación de firma deben ser robustos frente a hipotéticos intentos de falsificación. Los sistemas siempre deben trabajar con la posibilidad de que un falsificador tenga a su disposición toda la información posible para realizar una falsificación muy parecida a una firma genuina.
- **Baja permanencia temporal**: la firma de un individuo tiende a sufrir variaciones con el paso del tiempo.

2.2.1. Tipos de sistemas biométricos basados en firma manuscrita

En función del propósito final del sistema, existen dos configuraciones diferentes para los sistemas biométricos basados en firma manuscrita:

Sistemas biométricos de identificación

En este tipo de sistemas se busca conocer la identidad de un determinado usuario mediante comparaciones entre sus rasgos biométricos (que se introducen como entrada del sistema) y todos los rasgos biométricos almacenados en la base de datos del sistema, es decir, el sistema busca determinar la identidad del individuo al que le pertenece un determinado rasgo capturado por un sensor de entrada (en este caso, una firma manuscrita). Este tipo de sistemas conllevan un alto coste computacional ya que se comparan los rasgos biométricos del usuario de entrada con todos los rasgos almacenados en la base de datos (por lo tanto, el coste computacional del sistema dependerá del tamaño de su base de datos). Como salida, el sistema ofrece la identidad del usuario, en caso de que este ya hubiese sido previamente registrado en la base de datos.

Sistemas biométricos de verificación

Este tipo de sistema, a diferencia del anterior, recibe dos entradas: por un lado el rasgo biométrico del usuario y por otro lado una prueba de identidad del mismo (su nombre, un id, un nombre de usuario, una tarjeta, un email, etc.) y busca determinar si el usuario es efectivamente quien dice ser. En este caso, el sistema busca el usuario en cuestión dentro de la base de datos y compara su rasgo biométrico de entrada con los almacenados, por lo tanto, la salida es binaria: el usuario es quien dice ser si la comparación ha resultado exitosa o es un impostor en caso contrario. En este caso, el coste computacional es mucho más bajo debido a que únicamente se realiza una comparación.

Todo este proyecto ha sido llevado a cabo con un sistema biométrico de verificación, que será descrito más adelante, en este mismo capítulo. Para medir el rendimiento de estos sistemas se tienen en cuenta dos tipos de errores:

- **Falsa Aceptación (FA)**: este error hace referencia a los usuarios que han conseguido hacerse pasar por otros individuos sin que el sistema haya sido capaz de detectarlo (este tipo de errores se conocen también como *falsos positivos*).
- **Falso Rechazo (FR)**: este error hace referencia a los usuarios genuinos que el sistema considera impostores (de forma análoga al caso anterior, este tipo de errores se conocen como *falsos negativos*).

Mediante estos dos errores, junto con un umbral de decisión (habitualmente conocido como *threshold*), se definen dos parámetros de rendimiento: la **tasa de falsa aceptación (FAR)** y la **tasa de falso rechazo (FRR)**. Con estas dos tasas definimos el **Equal Error Rate (EER)**, que determina la tasa de error del sistema cuando se cumple la condición $FAR = FRR$. Las tasas FAR y FRR, junto con el EER, se representan por medio de las **curvas DET (Detection Error Trade-off)**.

2.3. Sistemas de verificación de firma manuscrita

En función de la información disponible, existen diferentes implementaciones para un sistema de verificación de firma manuscrita. Las más importantes son las dos siguientes [4]:

- **Sistemas basados en firma *on-line* o firma dinámica:** este tipo de sistemas se basa en la utilización de toda la información adquirida por el dispositivo de captura. De forma habitual, esta información comprende a las muestras de las coordenadas espaciales x e y , junto con la marca de tiempo de cada muestra e información adicional como el número de *pen-ups* (número de veces que el usuario ha levantado el bolígrafo de firmado tipo *stylus* o el dedo del dispositivo durante la elaboración de la firma), los niveles de presión en cada una de las muestras, etc. Ha quedado demostrado que este tipo de sistemas ofrecen mejor resultado gracias a que emplean una mayor cantidad de información, como quedó demostrado en multitud de publicaciones [5] [6] [7] [8].
- **Sistemas basados en firma *off-line* o firma estática:** este tipo de sistemas de verificación trabaja únicamente con la información extraída de imágenes estáticas de las firmas capturadas.

2.3.1. Sistemas de verificación de firma dinámica en función de las características de las firmas que utilizan

Dentro de los sistemas de verificación basados en firma dinámica podemos encontrar dos sistemas diferentes en función del tipo de características de las firmas que utilizan:

- **Sistemas basados en características globales:** este tipo de sistemas se basa en características extraídas a partir de la firma en su conjunto. Algunos ejemplos de estas características son la duración temporal de la firma, el número de *pen-ups* realizados, la velocidad media de la firma, etc. En la literatura se suele utilizar un conjunto de 100 características globales [9]. Las características globales a menudo se conocen como *global features*.
- **Sistemas basados en características locales:** este tipo de sistemas está basado en funciones temporales (y modificaciones de las mismas) capturadas durante el proceso de adquisición de una firma. Las funciones temporales capturadas durante la adquisición suelen ser las coordenadas espaciales x e y y la presión (aunque la presión es un dato que no siempre se encuentra disponible). Con estas funciones temporales iniciales se generan 23 funciones temporales nuevas, que se describen en el siguiente apartado. Las características locales a menudo se conocen como *local features*.

2.3.2. Tipos de falsificaciones

En las bases de datos de firmas manuscritas dinámicas que se encuentran en el estado del arte, existen dos tipos diferentes de falsificaciones:

- **Skilled forgeries:** en este primer tipo de falsificaciones, el usuario que va a realizar la falsificación tiene a su disposición la siguiente información: imagen de la firma que va a falsificar (y que tiene todo el tiempo del mundo para observarla tantas veces como quiera) y, en la mayoría de los casos, las dinámicas de firmado (es decir, la evolución de la firma en el tiempo).
- **Random forgeries:** en este segundo tipo de falsificaciones, un usuario cualquiera de la base de datos hace pasar su firma genuina por la firma genuina de otro usuario de la base de datos.

2.4. Sistema de verificación de firma manuscrita dinámica basado en *local features*

En este cuarto apartado se describe el funcionamiento del sistema biométrico de verificación de firma manuscrita basado en *local features* sobre el que se ha trabajado a lo largo de este Trabajo de Fin de Máster.

Como se ha comentado en la anterior sección, existen diferentes implementaciones para un sistema de verificación, sin embargo, en este trabajo se ha decidido utilizar un **sistema de verificación basado en funciones temporales**, más conocidas en la literatura como ***local features***. El sistema utilizado está basado en los trabajos [10] [11] y utiliza algunas modificaciones presentadas en [4].

Este sistema utiliza el **algoritmo DTW** (que se describirá más adelante) para realizar tanto el alineamiento como la comparación entre las firmas. Los principales motivos que han llevado a la selección de este algoritmo para implementar el sistema son los siguientes:

- Su coste computacional es bajo.
- No requiere de una gran base de datos de entrenamiento para ofrecer buenos resultados, como sí requieren otros enfoques alternativos, como los basados en *deep learning*.
- El buen rendimiento del algoritmo DTW hace que siga siendo un sistema de referencia en la verificación de firma manuscrita dinámica [12].

El conjunto de 23 *local features* con el que trabaja el sistema utilizado se muestra en la tabla 2.2, y ha sido seleccionado del total de 27 *local features* recogidas en [13], y es el mismo que se ha utilizado en otros estudios del estado del arte, como [12] [4].

Durante este proyecto se ha trabajado siempre con los siguientes 3 tipos de comparaciones entre diferentes firmas:

- **Comparaciones genuinas:** mediante DTW se calcula la distancia que hay entre 2 firmas genuinas de un determinado usuario.
- **Comparaciones impostoras (*skilled forgeries*):** mediante DTW se calcula la distancia que hay entre 1 firma genuina y 1 falsificación.
- **Comparaciones aleatorias (*random forgeries*):** mediante DTW se calcula la distancia que hay entre 1 firma genuina de un determinado usuario y 1 firma genuina de otro usuario.

#	Feature	Description
1	x-coordinate	x_n
2	y-coordinate	y_n
3	Pen-pressure	z_n
4	Path-tangent angle	$\theta_n = \arctan(\dot{y}_n/\dot{x}_n)$
5	Path velocity magnitude	$v_n = \sqrt{\dot{y}_n^2 + \dot{x}_n^2}$
6	Log curvature radius	$\rho_n = \log(1/k_n) = \log(\dot{v}_n/\dot{\theta}_n)$, where k_n is the curvature of the position trajectory
7	Total acceleration magnitude	$a_n = \sqrt{\dot{t}_n^2 + \dot{c}_n^2} = \sqrt{\dot{v}_n^2 + v_n^2 \dot{\theta}_n^2}$, where t_n and c_n are respectively the tangencial and centripetal acceleration components of the pen motion
8 - 14	First-order derivate of features 1-7	$\dot{x}_n, \dot{y}_n, \dot{z}_n, \dot{\theta}_n, \dot{v}_n, \dot{\rho}_n, \dot{a}_n$
15, 16	Second-order derivate of features 1, 2	\ddot{x}_n, \ddot{y}_n
17	Ratio of the minimum over the maximum speed over a 5-samples window	$v_n^r = \min v_{n-4}, \dots, v_n / \max v_{n-4}, \dots, v_n$
18, 19	Angle of consecutive samples and first order difference	$\alpha_n = \arctan((y_n - y_{n-1}) / (x_n - x_{n-1})) \dot{\alpha}_n$
20	Sine	$s_n = \sin(\alpha_n)$
21	Cosine	$c_n = \cos(\alpha_n)$
22	Stroke length to width ratio over a 5-samples window	$r_n^5 = \frac{\sum_{k=n-4}^{k=n} \sqrt{(x_k - x_{k-1})^2 + (y_k - y_{k-1})^2}}{\max x_{n-4}, \dots, x_n - \min x_{n-4}, \dots, x_n}$
23	Stroke length to width ratio over a 7-samples window	$r_n^7 = \frac{\sum_{k=n-6}^{k=n} \sqrt{(x_k - x_{k-1})^2 + (y_k - y_{k-1})^2}}{\max x_{n-6}, \dots, x_n - \min x_{n-6}, \dots, x_n}$

Tabla 2.2: Conjunto de *local features* utilizado en el presente proyecto. El punto situado sobre alguna de las características (e.g. \dot{x}_n), indica derivada en el tiempo. Tabla adaptada de [1].

Las **comparaciones genuinas** se estudian para poder asegurar que el sistema reconoce al usuario. Las **comparaciones impostoras** se estudian para evitar que el sistema reconozca como usuario a un impostor. Las **comparaciones aleatorias** se estudian para asegurar que el sistema no confunde las firmas de 2 usuarios diferentes.

Mediante el algoritmo DTW se alinean las 2 firmas que van a participar en la comparación y se calcula la distancia resultante. Mediante esta distancia se calcula el *score* final de la comparación, por medio de la ecuación 2.1, presentada en [14]:

$$score = e^{-D/K} \quad (2.1)$$

donde D representa la distancia mínima acumulada total entre las dos firmas que se están comparando y K es un factor de normalización que pondera el número de muestras que han sido alineadas en la comparación [15].

En este Trabajo de Fin de Máster se trabaja tanto con firmas introducidas mediante *stylus* como con firmas introducidas mediante el dedo. Debido a que la información relativa a la presión durante el firmado (*local features* 3 y 10) no se registra durante el proceso de captura de una firma introducida mediante el dedo, esta información no se ha utilizado tampoco en el caso de las firmas introducidas mediante *stylus*.

A continuación se describe de forma detallada el funcionamiento del algoritmo de alineamien-

to temporal de firmas DTW. Algunas de las ecuaciones y comentarios aportados en el siguiente apartado han sido extraídos de [4] y [11].

2.4.1. *Dynamic Time Warping* (DTW)

El algoritmo *Dynamic Time Warping* (en español, alineamiento temporal dinámico) o, simplemente, **DTW**, es un algoritmo utilizado para calcular el nivel de similitud existente entre dos secuencias temporales (en este Trabajo de Fin de Máster, todas las secuencias temporales son secuencias de muestras de una firma manuscrita, pero el algoritmo DTW funciona con cualquier otro tipo de secuencia temporal), que no tienen que tener necesariamente el mismo tamaño (de hecho, en la práctica es poco habitual encontrar dos versiones de firmas genuinas de un determinado usuario con una duración temporal idéntica y, por tanto, suelen tener diferente número de muestras), de hecho, la duración temporal de una firma no se considera como un factor relevante a la hora de realizar una comparación entre firmas. El algoritmo DTW consiste en encontrar el camino óptimo entre ambas secuencias temporales que minimice una medida de distancia entre ellas. El algoritmo DTW funciona siguiendo los siguientes pasos:

En primer lugar, se parte de dos secuencias temporales: X e Y :

$$X = x_1, x_2, \dots, x_i, \dots, x_I \quad (2.2)$$

$$Y = y_1, y_2, \dots, y_j, \dots, y_J \quad (2.3)$$

En segundo lugar, se define una medida de distancia entre ambas secuencias temporales (habitualmente se escoge la distancia conocida como **norma euclídea** o **norma vectorial**):

$$d(i, j) = ||x_i - y_j|| \quad (2.4)$$

Esta medida de distancia se calcula entre una muestra de cada una de las secuencias. En tercer lugar, se define el siguiente camino de alineamiento:

$$C = c_1, c_2, \dots, c_k, \dots, c_K \quad (2.5)$$

donde c_k representa una correspondencia (i, j) entre dos muestras concretas de las secuencias X e Y . El punto de partida del algoritmo, también conocido como condición inicial, es el siguiente:

$$g_1 = g(1, 1) = d(1, 1) * w(1) \quad (2.6)$$

donde g_k representa la distancia acumulada después de k iteraciones del algoritmo y $w(k)$ es un factor de ponderación que debe ser definido previamente. Para cada iteración, g_k es calculado según la siguiente ecuación:

$$g_k = g(i, j) = \min_{c_{k-1}} [g_{k-1} + d(c_k) * w(k)] \quad (2.7)$$

hasta alcanzar la distancia final (muestra final) I y J de ambas secuencias temporales. La distancia acumulada final se normaliza según la siguiente ecuación:

$$D(X, Y) = \frac{g_K}{\sum_{k=1}^K w(k)} \quad (2.8)$$

donde el término $\sum_{k=1}^K w(k)$ compensa el impacto generado por la longitud de las secuencias. El factor de ponderación w_k se define con el objetivo de limitar la correspondencia entre muestras de ambas secuencias temporales. Para el cálculo de la distancia acumulada en cada iteración sólo se permite una de las siguientes tres acciones:

$$g_k = g(i, j) = \min \begin{pmatrix} g(i, j-1) + d(i, j) \\ g(i-1, j-1) + 2d(i, j) \\ g(i-1, j) + d(i, j) \end{pmatrix} \quad (2.9)$$

La implementación mostrada en la ecuación 2.9 es una de las implementaciones más comunes del algoritmo DTW y es una de las que mejor rendimiento ofrece para el alineamiento temporal entre 2 firmas manuscritas, como se ha comentado anteriormente, y como quedó demostrado en [16].

2.4.2. Funcionamiento de un sistema de verificación de firma manuscrita basado en *local features*

Una vez descrito el funcionamiento del algoritmo DTW y una vez descritas las 23 *local features* que utiliza el sistema utilizado, en este apartado se describe el funcionamiento del sistema de verificación de firma manuscrita así como de todas sus etapas. Esta sección ha sido adaptada de [4] y de [11].

Adquisición de los datos

En esta primera etapa, se captura la información de la firma genuina del usuario, mediante un dispositivo conocido como sensor. La información capturada suele ser la siguiente: muestras de las coordenadas espaciales x e y y marca del tiempo de cada una de las muestras. Esta información se captura independientemente del dispositivo utilizado y del método de introducción de la firma (*stylus* o dedo). En el caso de que el dispositivo utilizado sea un *stylus*, adicionalmente se captura la siguiente información: niveles de presión de cada muestra, número de *pen-ups* y orientación del *stylus*.

El dispositivo de captura almacena los datos capturados en un fichero de texto, habitualmente un fichero con extensión *.txt*.

Pre-procesamiento de los datos

Con el objetivo de evitar o minimizar la cantidad de ruido que es introducido en el sistema, es habitual realizar una etapa de pre-procesado de los datos, para eliminar errores como muestras repetidas, datos atípicos, etc.

Extracción de *local features*

Una vez han sido pre-procesados los datos de entrada y se han eliminado posibles errores, la siguiente etapa consiste en la extracción de las 23 *local features* descritas en la tabla 2.2.

En el caso de las firmas introducidas mediante el *stylus*, la función temporal de la presión que se ha capturado se utiliza para el cálculo de las *local features* 3 y 10. Para el caso de las firmas introducidas mediante el dedo, estas *local features* valen siempre 0.

Las muestras de las funciones temporales de las coordenadas espaciales x e y se utilizan para calcular las 21 *local features* restantes.

Por motivos de privacidad, los cálculos necesarios para la obtención de las 23 *local features* han sido omitidos en esta memoria.

Alineamiento y cálculo de la similitud entre firmas

Mediante el algoritmo DTW se alinean las dos firmas a comparar y se obtiene la distancia final óptima de la comparación.

Para la comparación entre firmas no se utilizan las 23 *local features*, se utilizan subconjuntos de ellas que han sido encontrados como los más óptimos en función de cada situación. Para la extracción de estos subconjuntos se utilizan algoritmos de selección de características, habitualmente el algoritmo *Sequential Forward Floating Search* (SFFS) [17].

Cálculo de *scores* y resultado final

Una vez conocida la distancia final óptima de la comparación entre las firmas, se calcula y normaliza el *score* mediante la ecuación 2.1. La normalización del *score* al intervalo $[0, 1]$ se efectúa para evitar que firmas de mayor duración temporal obtengan *scores* más altos (las técnicas de normalización de *scores* más utilizadas se estudian y describen en [18]).

Si dos firmas son exactamente iguales, el *score* final de la comparación será igual a 1. Si dos firmas son completamente diferentes, el *score* final será igual a 0.

Mediante el *score* final y un umbral de decisión (más conocido como *threshold*), se decide si las firmas corresponden al mismo usuario (ambas firmas son genuinas) o si alguna de ellas es una falsificación.

2.5. Más allá de DTW: Técnicas basadas en *deep learning*

Las técnicas basadas en *deep learning* han conseguido excelentes resultados en la realización de multitud de tareas informáticas. Sin embargo, en algunas tareas, como la verificación de firmas manuscritas, no se ha podido explotar todo el potencial del *deep learning*, debido a que no existen en el estado del arte grandes bases de datos que faciliten el entrenamiento de sistemas basados en *deep learning* que ofrezcan mejores resultados que los presentados por los sistemas tradicionales de verificación de firma manuscrita. Gracias a la publicación en [19] de la base de datos *DeepSignDB*, de la que se hablará en el próximo capítulo, se han podido desarrollar algunos sistemas de verificación basados en *deep learning* que mejoran el rendimiento de los sistemas tradicionales.

En los 2 últimos años se han realizado avances significativos en la verificación de firma manuscrita mediante *deep learning*. En [20] se propone un sistema (descrito en la figura 2.1), nombrado por sus autores como *Time-Aligned Recurrent Neural Networks* (TA-RNNs) que mejora tanto los resultados obtenidos por los sistemas de verificación tradicionales, como otras aproximaciones basadas en *deep learning* (e.g., [21]) tal y como queda demostrado en la tabla 2.3.

El sistema basado en TA-RNNs también ha ofrecido mejores resultados que algunos estudios del estado del arte basados en *deep learning*, que trabajan con firmas introducidas mediante el dedo, sin embargo, aún no ha conseguido mejorar el rendimiento de todos ellos, como queda reflejado en la tabla 2.4, donde se muestra una comparativa entre el rendimiento de las TA-RNNs

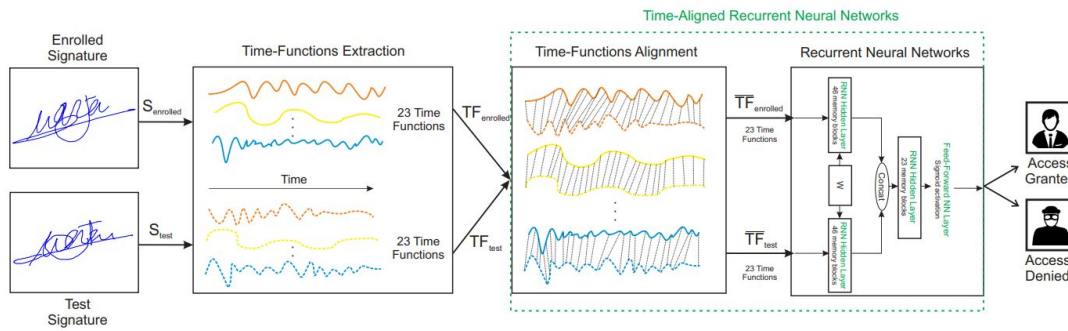


Figura 2.1: Arquitectura del sistema de verificación de firma manuscrita basado en *Time-Aligned Recurrent Neural Networks* (TA-RNNs).

Sistema	Usuarios de entrenamiento	Útil de escritura	Firmas de entrenamiento por usuario	Rendimiento (EER)
Tolosana <i>et al.</i> (2018) [21]	300	Stylus	1	Skilled = 6.8 % Random = 5.4 %
			4	Skilled = 5.5 % Random = 2.9 %
TA-RRNs (2020) [20]	1084	Stylus	1	Skilled = 4.2 % Random = 1.5 %
			4	Skilled = 3.3 % Random = 0.6 %

Tabla 2.3: Comparativa del rendimiento (EER) ofrecido por un enfoque tradicional de verificación y un nuevo enfoque basado en *deep learning*. Los términos *Skilled* y *Random* hacen referencia respectivamente a los tipos de falsificaciones *skilled* y *random forgeries*.

y otros dos sistemas de verificación basados en *deep learning*, uno con un rendimiento superior y otro con un rendimiento inferior.

Además de los enfoques basados en redes neuronales recurrentes comentados, en el estado del arte pueden encontrarse estudios que propone alternativas conjuntas entre DTW y redes neuronales (e.g., [24] y [25]).

Los autores de [24] proponen una arquitectura siamesa de 2 redes neuronales convolucionales (CNNs) que realizan un prealineamiento de las firmas antes de que ambas sean introducidas como entradas del algoritmo DTW. Mediante esta arquitectura, los autores consiguen mejorar el EER obtenido en la base de datos *MCYT* del 5 % al 1 %.

En [25] se propone una arquitectura siamesa basada en CNNs parecida, pero cuyos pasos se realizan de forma inversa: primero se realiza un prealineamiento mediante DTW y las *local features* de ambas firmas, que ya están alineadas se introducen como entrada de las CNNs. En este caso se consigue reducir el EER de verificación obtenido en la base de datos *MCYT* hasta el 0.5 %.

La conclusión que puede extraerse tras el estudio de las diferentes técnicas de alineamiento basadas en *deep learning* que pueden encontrarse en el estado del arte es que estas técnicas permiten mejorar el rendimiento de verificación de los sistemas tradicionales. Adicionalmente, la combinación de estas técnicas de *deep learning* con el algoritmo DTW ofrece también resultados superiores a los del estado del arte y resulta una línea de investigación de gran interés para el futuro.

Sistema	Usuarios de entrenamiento	Útil de escritura	Firmas de entrenamiento por usuario	Rendimiento (EER)
Lai and Jin (2018) [22]	70	Finger	5	Skilled = 10.9 % Random = 0.6 %
Li <i>et al.</i> (2019) [23]	70	Finger	1	Skilled = 16.1 % Random = Sin datos
TA-RNNs (2020) [20]	1084	Finger	1	Skilled = 13.8 % Random = 1.8 %
			4	Skilled = 11.3 % Random = 1.0 %

Tabla 2.4: Comparativa del rendimiento (EER) ofrecido por dos enfoques de verificación basados en *deep learning* y un nuevo enfoque basado en *deep learning*. Los términos *Skilled* y *Random* hacen referencia respectivamente a los tipos de falsificaciones *skilled* y *random forgeries*.

3

Bases de datos de firma manuscrita.

3.1. Bases de datos de firma manuscrita

De forma análoga a otras tecnologías similares, los sistemas biométricos de verificación de firma manuscrita dinámica han sufrido una notable evolución en los últimos años [19]: inicialmente se utilizaban dispositivos específicos para implementarlos, como las tabletas digitalizadoras Wacom (como la que se muestra en la figura 3.1), pero en la actualidad, la gran popularización de los *smartphones* han ampliado el espectro de posibilidades en cuanto a formas de adquisición. Estas nuevas formas de adquisición y captura de firmas se caracteriza por los siguientes factores: por un lado, el útil de escritura ya no es necesario que sea un dispositivo específico como un bolígrafo tipo *stylus*, si no que las firmas se introducen mediante el dedo (lo que, en general, no permite alcanzar el mismo nivel de detalle que el *stylus*). Por otro lado, el escenario en el que se realiza la adquisición de la firma ya no es necesario que sea un escenario controlado, como la oficina de una entidad bancaria, si no que puede ser cualquier escenario móvil de la vida cotidiana, incluyendo situaciones como viajes en transporte público, etc.

Existen en la literatura diferentes arquitecturas e implementaciones de sistemas de verificación de firma manuscrita basados en *deep learning*, que han presentado buenos resultados, sin embargo, estos aún no gozan de una gran popularidad debido a que requieren de un gran conjunto de datos de entrenamiento (que a menudo no está disponible) para desarrollarse [9] [5]. Las bases de datos utilizadas en el presente proyecto son un subconjunto de la base de datos *DeepSignDB*, presentada en [19], y que cuenta con diferentes bases de datos de firma dinámica en su interior y la base de datos *MobileTouchDB*, presentada en [3].

3.2. La base de datos *DeepSignDB*

Las principales características de la base de datos *DeepSignDB* se listan a continuación:

- Es una base de datos formada por la unión de las principales bases de datos de firma dinámica presentes en el estado del arte.
- Cuenta con más de 70000 firmas, introducidas tanto mediante el uso de un útil de escritura específico, como un bolígrafo tipo *stylus*, como introducidas mediante el dedo.



Figura 3.1: Ejemplo de tableta digitalizadora Wacom y bolígrafo *stylus*.

- Contiene en total 1526 usuarios diferentes.
- Para la adquisición de la base de datos se han considerado 2 escenarios de captura diferentes (un escenario controlado tipo oficina y un escenario móvil).
- La base de datos cuenta con un total de 8 dispositivos de captura diferentes (5 dispositivos de uso específico y 3 dispositivos móviles comerciales).
- La base de datos cuenta también con diferentes tipos de falsificaciones y diferentes números de sesiones de captura, lo que permite también estudiar la robustez del sistema desarrollado frente a intentos de falsificación y frente a posibles variaciones de la firma con el tiempo.

La base de datos *DeepSignDB* está formada por cuatro de las bases de datos más populares del estado del arte: *MCYT* [26], *BiosecurID* [27], *Biosecure DS2* [28] y *e-BioSign* [12]. Sin embargo, en el presente Trabajo de Fin de Máster únicamente se ha utilizado la base de datos *e-BioSign*, que a su vez está formada por 2 *datasets*: DS1 y DS2.

Únicamente se ha tenido en cuenta la base de datos *e-BioSign* debido a que es la única que cuenta tanto con firmas introducidas mediante *stylus* como firmas introducidas mediante el dedo, para los mismos usuarios, lo que permite realizar los experimentos que se quieren realizar en el presente proyecto. A continuación se describe la base de datos *e-BioSign*, dividida en sus 2 *datasets*:

3.2.1. *e-BioSign* DS1

La base de datos *e-BioSign* DS1 está formada por firmas capturadas mediante 5 dispositivos de captura diferentes: tres de ellos diseñados específicamente para la captura de firmas manuscritas (tabletas digitalizadoras Wacom STU-500, Wacom STU-530 y Wacom DTU-1031) y los dos restantes son *smartphones* comerciales (Samsung ATIV 7 y Samsung Galaxy Note 10.1).

En los 5 dispositivos comentados se utilizó para la captura de firmas un útil de escritura tipo *stylus* y, adicionalmente, en los dos *smartphones* se capturaron firmas introducidas mediante el dedo.

Para la captura se efectuó el mismo protocolo en el caso de los 5 dispositivos: se situó el dispositivo sobre una mesa y se permitió al usuario rotarlo hasta encontrar la posición más cómoda para la realización de la firma.

La base de datos cuenta con un total de 65 usuarios, para cada uno de los cuales, y para el caso de cada dispositivo, se capturaron 8 firmas genuinas y 6 falsificaciones (en el caso de los *smartphones*, se tienen también 8 firmas genuinas y 6 falsificaciones adicionales por usuario y por dispositivo).

Todas las firmas se adquirieron en dos sesiones de captura, con una separación temporal entre ellas de 3 semanas. Para el caso de las firmas introducidas mediante *stylus* se capturó la siguiente información: coordenadas espaciales x e y , niveles de presión, marcas de tiempo e información sobre las trayectorias de los *pen-ups* (momentos en los que el usuario levanta el *stylus* de la pantalla). Para el caso de las firmas introducidas mediante el dedo únicamente se capturaron muestras de las coordenadas espaciales y marcas de tiempo (los dispositivos móviles no permiten la captura del resto de la información).

En cuanto a las falsificaciones, se realizaron dos tipos diferentes: para todos los usuarios se generaron falsificaciones en las que el falsificador únicamente tenía disponible la imagen final de la firma y falsificaciones en las que, además de la imagen final de la firma, también se tenían disponibles las dinámicas de firmado (es decir, la evolución de la firma en el tiempo). Durante el proceso de falsificación de la firma los falsificadores podían observar la información disponible todas las veces y durante todo el tiempo que desearan.

3.2.2. *e-BioSign* DS2

La base de datos *e-BioSign* DS2 se capturó con un protocolo de adquisición similar al utilizado para la captura de la base de datos *e-BioSign* DS1.

La base de datos *e-BioSign* DS2 cuenta con 3 dispositivos de captura de firmas diferentes: un dispositivo de uso específico, una tableta Wacom STU-530 y dos dispositivos tipo *smartphone*, un Samsung Galaxy Note 10.1 y un Samsung Galaxy S3.

Las firmas capturadas mediante el dispositivo Wacom STU-530 se realizaron en un escenario controlado tipo oficina, en el que se situaba la tableta sobre una mesa de escritorio y se permitía a los usuarios rotarlo hasta alcanzar la disposición más cómoda para realizar la firma. Las firmas capturadas mediante los dos *smartphones* se realizaron en un escenario que buscaba simular una situación cotidiana en la que los usuarios firmaron en el *smartphone* mientras se encontraban sentados en una silla.

Para el caso de la tableta Wacom sólo se capturaron firmas introducidas mediante *stylus*, mientras que para los 2 *smartphones* se utilizó el dedo para introducir la firma.

En total, la base de datos *e-BioSign* DS2 cuenta con un total de 81 usuarios, cuyas firmas se recogieron en 2 sesiones de captura, separadas por 3 semanas. Para cada usuario y cada dispositivo se capturaron 8 firmas genuinas y 6 falsificaciones. La información registrada para las firmas introducidas mediante *stylus* y mediante dedo es exactamente la misma que en la base de datos *e-BioSign* DS1. En cuanto a las falsificaciones, en este caso únicamente se realizaron falsificaciones en las que se tenía disponible tanto la imagen final de la firma como la información relativa a las dinámicas de firmado.

Un resumen con la información principal de los 2 *datasets* de la base de datos *e-BioSign* se muestra en la tabla 3.1.

	Usuarios	Sesiones	Disps.	Firmas genuinas	Falsificaciones
e-BioSign DS1	65	2	5	8 stylus (+8 dedo)	6 stylus (+6 dedo)
e-BioSign DS2	81	2	3	8 stylus (+8 dedo)	6 stylus (+6 dedo)

Tabla 3.1: Resumen con las principales características de los 2 *datasets* de la base de datos *e-BioSign*.

3.3. La base de datos *MobileTouchDB*

Como se ha comentado anteriormente, la amplia comercialización de los teléfonos móviles inteligentes de los últimos años ha abierto la posibilidad de desarrollar sistemas de verificación sin necesidad de utilizar una tableta digitalizadora. La captura de firmas mediante *smartphones* cuenta con las siguientes dos características:

- Ya no es necesaria la utilización de un útil de escritura específico, como el lápiz tipo *stylus*, como era el caso de las tabletas Wacom, sino que ahora se introduce la firma mediante el dedo. Este hecho conlleva un inconveniente, mediante el dedo no es posible alcanzar el mismo nivel de detalle que mediante un lápiz tipo *stylus*, por lo que las firmas introducidas tienen una menor calidad.
- El escenario de captura de las firmas ya no tiene que ser un escenario controlado (como por ejemplo una oficina), si no que puede ser cualquier escenario cotidiano (como por ejemplo durante un viaje en el transporte público).

A pesar de la rápida popularización de los *smartphones*, apenas existen bases de datos de firmas introducidas mediante el dedo, lo que dificulta enormemente el desarrollo de sistemas de verificación de este tipo [9] [5].

3.3.1. Introducción y contexto

La base de datos **MobileTouch** fue presentada por primera vez en [3], en mayo de 2019, con el objetivo de ofrecer a la comunidad una nueva base de datos con información de firmas introducidas con el dedo (además de contar con varias firmas por usuario, incluye información sobre la escritura manuscrita de dígitos y letras) que permita el desarrollo y entranamiento de nuevos sistemas de verificación, que siempre han estado muy limitados por la poca cantidad de datos disponible.

La base de datos está formada por 6 sesiones de captura diferentes, separadas temporalmente por 2 días (salvo el caso de la sesión 3 a la 4, que están separadas por 7 días). En cada sesión de captura se registraba la siguiente información:

- Dos firmas genuinas.
- Dígitos del 0 al 9.
- Todas las letras minúsculas del abecedario.
- Todas las letras mayúsculas del abecedario.
- Ocho símbolos, como el símbolo de equivalencia o el de interrogación.
- Una composición formada por 4 números.

Dado que el propósito de este trabajo es el estudio de la firma manuscrita, de toda la información disponible se han seleccionado únicamente las dos firmas genuinas de cada sesión. De cada firma se ha registrado la siguiente información:

- Coordenadas x e y de cada muestra capturada de la firma.
- Marca de tiempo de cada muestra.
- Diámetro del área apoyada del dedo en la pantalla para cada muestra.
- Las tres coordenadas espaciales (x, y, z) del giroscopio del dispositivo móvil para cada muestra.
- Las tres coordenadas espaciales del acelerómetro del dispositivo móvil para cada muestra.

Es importante destacar que no todos los dispositivos móviles utilizados (en total 94 modelos de *smartphone* diferentes) para la captura de la base de datos contaban con la posibilidad de registrar las coordenadas espaciales de giroscopio y acelerómetro, por lo que esta información no está disponible en la totalidad de usuarios y no se va a tener en cuenta en este trabajo.

3.3.2. Pre-procesado de la base de datos

El autor de la base de datos únicamente capturó las firmas, pero no utilizó esa información para llevar a cabo ningún estudio. Inicialmente, en la base de datos hay un total de 217 usuarios que cuentan con sus firmas genuinas registradas, pero fue necesario llevar a cabo una etapa de pre-procesado de las firmas de cada usuario para garantizar la calidad de la información capturada y eliminar errores.

El pre-procesado se llevó a cabo por autor del presente Trabajo de Fin de Máster, mediante la visualización individual de todas las firmas, y se eliminaron en total 72 usuarios, principalmente por alguno de los siguientes tres motivos:

- Se detectó que había habido algún error en la captura de alguna sesión.
- El usuario había realizado firmas diferentes a lo largo de las sesiones.
- El usuario dejó vacía la pantalla de captura de la firma o hizo simplemente una línea o trazo simple en ella.

Tras este proceso de pre-procesado y limpieza, la base de datos pasó a contar únicamente con 145 usuarios, pero todos ellos con 6 sesiones de captura (12 firmas en total) registradas correctamente.

Para el desarrollo de un sistema biométrico de verificación es poco útil contar únicamente con firmas genuinas de los usuarios, porque resulta de vital importancia proteger al sistema frente a potenciales impostores. Por este motivo, se decidió **generar falsificaciones** para los usuarios 145 usuarios de la base de datos seleccionados tras el pre-procesado de la misma.

3.4. Generación de falsificaciones para *MobileTouchDB*

A la hora de desarrollar un sistema biométrico se debe tener en cuenta que sea robusto frente a dos tipos de falsificaciones (los mismos tipos de falsificaciones descritos en la sección 2.3.2. de la presente memoria):

- **Falsificaciones aleatorias:** en la literatura se conocen como *random forgeries*. En este tipo de falsificaciones un usuario cualquiera de la base de datos trata de hacer pasar su firma genuina por la firma genuina de otro usuario.
- **Falsificaciones habilidosas:** en la literatura se conocen como *skilled forgeries*. En este tipo de falsificaciones, el usuario que va a realizar la falsificación tiene a su disposición mucha información (a menudo, toda la información) sobre la firma a falsificar. Esto involucra la imagen final de la firma o las dinámicas de firmado (la evolución de la firma a lo largo del tiempo).

El estudio de las *skilled forgeries* es de especial importancia a la hora de evaluar el rendimiento de un determinado sistema, por lo que a lo largo de este trabajo es en este tipo de falsificaciones en las que se ha hecho hincapié.

Como se ha comentado anteriormente, la base de datos MobileTouchDB no contaba con falsificaciones de las firmas genuinas, por lo que fue necesario generarlas. Para generarlas se seleccionó a cuatro falsificadores, todos ellos con diferentes niveles de conocimiento sobre el funcionamiento de la firma manuscrita y se les pidió que generasen dos firmas de los dos siguientes tipos de falsificaciones:

- ***Skilled forgeries* estáticas:** en este primer tipo de falsificaciones, los falsificadores únicamente tuvieron a su disposición la imagen final de cada firma y, con ella, debían realizar la falsificación.
- ***Skilled forgeries* dinámicas:** en este segundo tipo de falsificaciones, los falsificadores disponían de un programa que les mostraba la evolución de la firma en el tiempo, lo que les permitía percibir información como el orden en el que se realizan los trazos o la velocidad de firmado, aspectos que no es posible conocer en el primer tipo de falsificaciones. En la figura 3.2 se muestran diferentes etapas de la visualización de las dinámicas de firmado de una firma de ejemplo.

3.4.1. Protocolo de generación de las falsificaciones

Para la adquisición de las falsificaciones se utilizó una modificación de la misma aplicación Android que utilizó el autor de [3] para generar la base de datos *MobileTouchDB*.

Los cuatro usuarios contactados para realizar las falsificaciones son miembros del grupo de investigación *Biometrics and Data Pattern Analytics* (BiDA Lab) de la Universidad Autónoma de Madrid (UAM) y todos ellos tienen conocimientos sobre el funcionamiento y las características de la firma manuscrita como rasgo biométrico (es decir, conocimientos superiores a la media de la población), por lo que las falsificaciones realizadas son sensiblemente de mayor calidad que las realizadas por un falsificador común.

En total se realizaron cuatro sesiones de falsificación (dos sesiones para cada tipo de falsificación), y en cada sesión se falsificó una firma genuina de cada uno de los 145 usuarios de la base de datos. La separación temporal entre cada sesión fue de una semana.

3.4.2. Generación de las *skilled forgeries* estáticas

Para la generación de las *skilled forgeries* estáticas, los falsificadores recibieron una guía (en formato PDF) de uso de la aplicación Android junto con una descripción de cómo debían

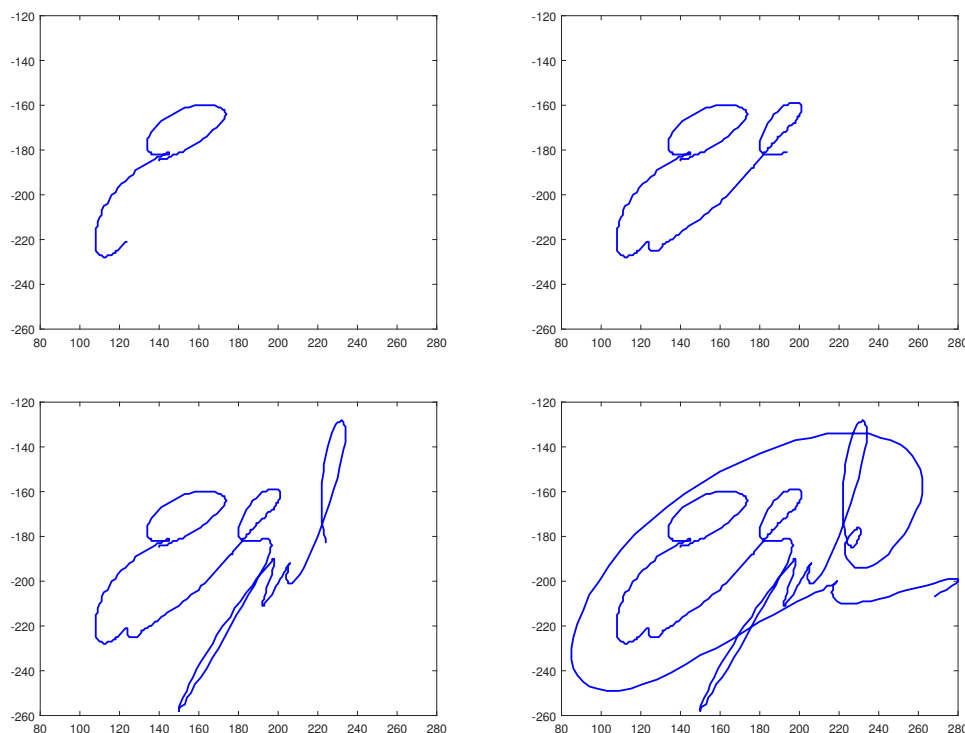


Figura 3.2: Ejemplos de las dinámicas de firmado (evolución de una firma en el tiempo) de una determinada firma de ejemplo.

realizar las falsificaciones y junto con las imágenes de todas las firmas a falsificar (estas imágenes se recopilaban, a tamaño grande, en un único documento PDF, para facilitar la labor de los falsificadores).

La aplicación Android va pidiendo al usuario que falsifique en orden cada una de las firmas de la base de datos. El usuario puede visualizar la firma a falsificar todo el tiempo que desee y, si no queda conforme con el resultado, se le permite repetir la falsificación todas las veces que sea necesario.

En la figura 3.3 se muestra a modo de ejemplo una firma genuina de un usuario de la base de datos *MobileTouchDB* (imagen izquierda) y una de las *skilled forgeries* estáticas generadas (imagen derecha). Puede observarse que, aunque existen ciertas diferencias entre ambas firmas, la calidad de la falsificación es elevada.

3.4.3. Generación de las *skilled forgeries* dinámicas

Para la generación de las *skilled forgeries* dinámicas, los falsificadores contaban, además de con toda la información ya disponible para el caso de las *skilled forgeries* estáticas, con un programa que permitía visualizar en vídeo la evolución de las dinámicas de firmado, tal y como se ha mostrado en la figura 3.2.

De nuevo, la aplicación Android va pidiendo al usuario que falsifique en orden cada una de las firmas de la base de datos. El usuario puede visualizar tanto la firma a falsificar como sus dinámicas de firmado todo el tiempo que desee y, si no queda conforme con el resultado, se le permite repetir la falsificación todas las veces que sea necesario.

En la figura 3.4 se muestra de nuevo, la una firma genuina del mismo usuario de la base de

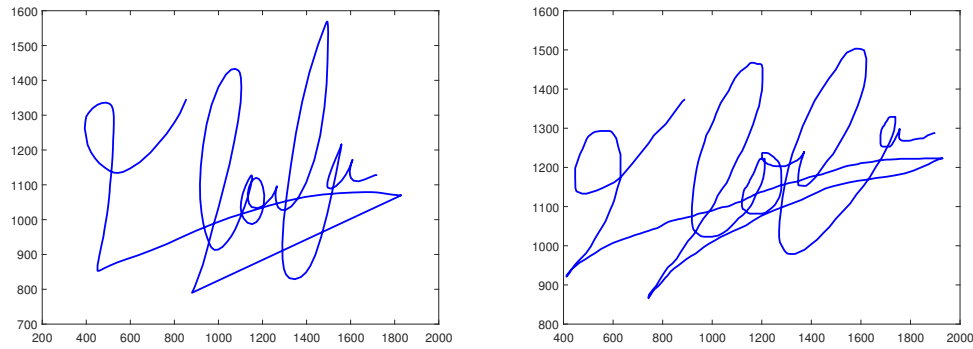


Figura 3.3: Ejemplo de una firma genuina de la base de datos *MobileTouchDB* (imagen izquierda) y una *skilled forgery* estática de ejemplo.

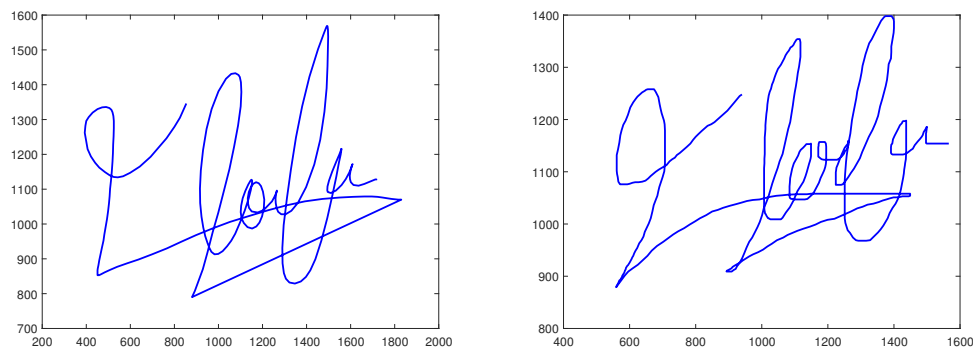


Figura 3.4: Ejemplo de una firma genuina de la base de datos *MobileTouchDB* (imagen izquierda) y una *skilled forgery* dinámica de ejemplo.

datos *MobileTouchDB* que en el caso anterior (imagen izquierda) y una de las *skilled forgeries* dinámicas generadas (imagen derecha). Puede observarse en este caso que las diferencias entre ambas firmas son muy leves, lo que es signo de que las *skilled forgeries* dinámicas generadas son de una calidad muy alta.

3.4.4. Pre-procesado de las falsificaciones generadas y eliminación de usuarios repetidos

Tras la generación de todas las falsificaciones, se realizó un pre-procesado mediante inspección visual de todas las firmas para asegurar la calidad de la información adquirida y eliminar posibles errores. Durante esta etapa de pre-procesamiento se detectaron los siguientes 2 problemas:

- Dos de los falsificadores habían sido parte del grupo de usuarios que generaron las firmas genuinas de *MobileTouchDB*.
- De los 145 usuarios disponibles, existen 6 usuarios repetidos (para incentivar la participación en la creación de la base *MobileTouchDB*, los autores sortearon entre los usuarios un premio, lo que hizo que algún usuario participase 2 veces en la adquisición de firmas para aumentar sus probabilidades de ganar).

Debido a que dos de los falsificadores habían sido parte del grupo de usuarios que generaron

las firmas genuinas de *MobileTouchDB*, durante la falsificación de sus firmas no estaban realizando una falsificación, sino una versión de su firma genuina. Para solucionar este problema se les pidió que cada uno de ellos realizase las falsificaciones de la firma genuina del otro usuario dos veces, de forma que al final se obtuvo el mismo número de falsificaciones para todos los usuarios.

Los 6 usuarios repetidos de la base de datos fueron eliminados, de forma que finalmente se obtuvo una base de datos con un total de 139 usuarios, con 12 firmas genuinas y 16 falsificaciones (8 *skilled forgeries* estáticas y 8 *skilled forgeries* dinámicas) por usuario.

4

Método Propuesto

En este capítulo se describe el método propuesto para la detección de los trazos más estables de la firma genuina de un usuario y su posterior utilización para la mejora del rendimiento de los sistemas de verificación.

Definimos **trazos** y **muestras estables** como aquellos trazos y muestras de la firma genuina de un usuario que cuentan con menores variaciones intra-clase (es decir, trazos y muestras que aparecen de forma similar en diferentes versiones de la firma genuina de un determinado usuario) y que, por lo tanto, su distancia DTW es muy pequeña (una distancia DTW pequeña implica que el *score* de la comparación ha sido muy próximo a 1).

4.1. Sistema propuesto

Los sistemas tradicionales de verificación de firma manuscrita funcionan de la siguiente forma: dadas 2 firmas (que pueden ser o 2 firmas genuinas o 1 firma genuina y 1 falsificación) se calcula el *score* de la comparación entre ellas mediante el algoritmo DTW. Si las dos firmas son genuinas lo esperado es que el *score* sea muy próximo a 1. Si una de las firmas es una falsificación, lo esperado es que el *score* sea muy próximo a 0.

El sistema propuesto en este Trabajo de Fin de Máster introduce una modificación a los anteriores sistemas: se calcula también el *score* de la comparación mediante DTW entre los trazos más estables de ambas firmas. La premisa con la que trabaja el sistema (y como quedará demostrado en el capítulo de experimentos de la presente memoria) es que existen regiones estables en la firma genuina de un usuario que permiten caracterizarla mejor y, de esta forma, mejorar el rendimiento del sistema a la hora de detectar falsificaciones.

A lo largo de los próximos apartados del presente capítulo se describen los métodos utilizados para la extracción de los trazos más estables de una firma, así como otros métodos alternativos que se han estudiado, pero que finalmente no han sido integrados en el sistema propuesto.

4.2. Segmentación de una firma en trazos mediante su perfil de velocidad

En este apartado se describe el sistema de extracción de trazos utilizado en el sistema propuesto. La extracción de trazos se realiza en base al perfil de velocidad, método presentado en [29], que a su vez está basado en el modelo presentado en [30]. El procedimiento para la extracción del perfil de velocidad de una firma es el siguiente:

1. División de la firma en dos estados según si el *stylus* o el dedo está en contacto con la pantalla (se está realizando un trazo) o se encuentra en el aire (no se está realizando un trazo). Este paso se realiza para evitar que no se consideren como un mismo trazo dos trazos separados por un momento en el que el útil de escritura está en el aire.
2. Para cada una de las muestras de las coordenadas espaciales x e y se calcula el vector de velocidad en ese punto (v_n) según la siguiente ecuación (las variables \dot{x}_n y \dot{y}_n denotan la primera derivada entre muestras consecutivas):

$$v_n = \sqrt{\dot{x}_n^2 + \dot{y}_n^2} \quad (4.1)$$

3. Una vez calculadas todas las velocidades, se divide la firma en trazos utilizando la media y la desviación típica de la velocidad.

Existen las siguientes 3 opciones a la hora de dividir en regiones el espacio de velocidades usando la media y la desviación típica. En función de la opción seleccionada se obtendrán trazos de mayor o menor tamaño:

- **División en trazos grandes:** para dividir una firma en trazos grandes, se particiona el espacio de velocidades en 2 regiones: las velocidades que están por encima de la media y las velocidades que están por debajo de la media (puede observarse un ejemplo de una partición del espacio de velocidades de este tipo en la imagen superior de la figura 4.1).
- **División en trazos medianos:** para dividir una firma en trazos medianos, se particiona el espacio de velocidades en 3 regiones: las velocidades que están por encima de la media más la desviación típica, las velocidades que están por debajo de la media menos la desviación típica y las velocidades que están entre la media más la desviación típica y la media menos la desviación típica (puede observarse un ejemplo de una partición del espacio de velocidades de este tipo en la imagen central de la figura 4.1).
- **División en trazos pequeños:** para dividir una firma en trazos pequeños, se particiona el espacio de velocidades en 4 regiones: las velocidades que están por encima de la media más la desviación típica, las velocidades que están por debajo de la media menos la desviación típica, las velocidades mayores que la media, pero menores que la media más la desviación típica y las velocidades menores que la media, pero mayores que la media menos la desviación típica (puede observarse un ejemplo de una partición del espacio de velocidades de este tipo en la imagen inferior de la figura 4.1).

La media y la desviación se utilizan para dividir el espacio de velocidades en regiones, tal y como se indica en la figura 4.1. Cuando la velocidad pasa de una región a otra, se establece un nuevo trazo (con algunas restricciones adicionales, como por ejemplo, número mínimo de muestras por trazo para, evitar trazos demasiado pequeños).

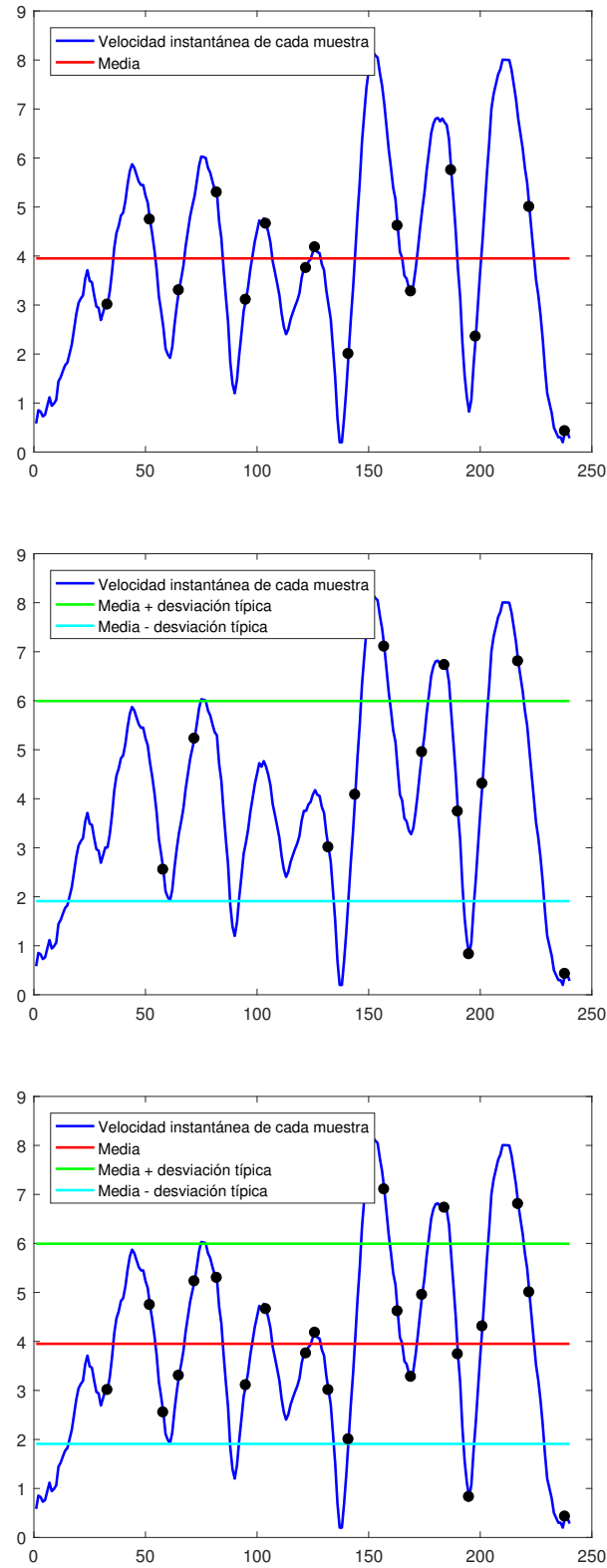


Figura 4.1: División del espacio de velocidades para generar trazos grandes (imagen superior), trazos medianos (imagen central) y trazos pequeños (imagen inferior). Los puntos negros indican los cambios de trazos.

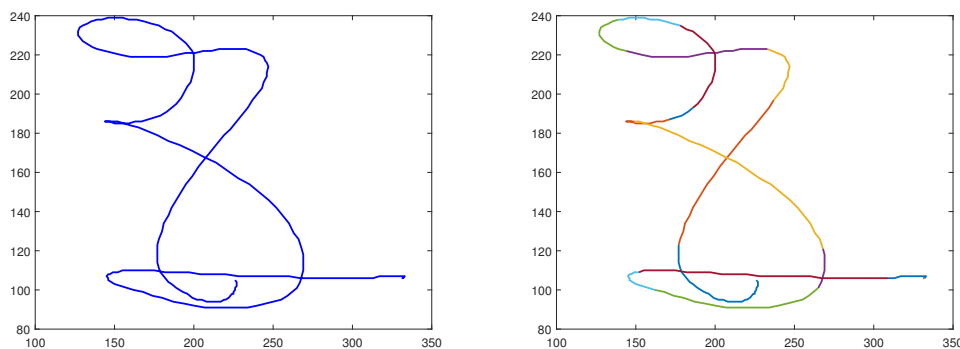


Figura 4.2: Ejemplo de firma manuscrita (imagen izquierda) y su descomposición en trazos mediante el perfil de velocidad (imagen derecha).

En la figura 4.2 se muestra un ejemplo de una firma (imagen izquierda) y su descomposición en trazos mediante la extracción del perfil de velocidad (imagen derecha). Un aspecto importante a destacar sobre la división en trazos mediante el perfil de velocidad es que no es estable a lo largo de las diferentes firmas genuinas de un usuario, lo que implica que el número de trazos en los que se divide las difentes firmas de un determinado usuario es diferente.

4.2.1. Emparejamiento de trazos entre firmas genuinas

En el capítulo 2 de la presente memoria se comentó que uno de los aspectos negativos de la firma manuscrita como rasgo biométrico es el hecho de que tiene baja permanencia temporal, es decir, la firma genuina de un individuo tiende a sufrir variaciones a lo largo del tiempo. Estas variaciones suponen una dificultad adicional a la hora de discernir qué firmas de un usuario son genuinas y cuáles no.

En la figura 4.3 se muestran dos firmas genuinas de un determinado usuario de la base de datos *e-BioSign* DS1, junto con su división en trazos. Cualquier observador puede detectar diferencias evidentes entre ambas firmas y en el número de trazos en los que ha sido dividida según su perfil de velocidad (28 trazos para el caso de la firma izquierda y 32 trazos para el caso de la firma derecha). Aunque existen ciertas diferencias entre ambas firmas, es posible apreciar también similitudes importantes entre sus trazos (a modo de ejemplo, el lazo superior izquierdo de ambas firmas es bastabte similar).

Como puede observarse en la figura 4.3, el número de trazos en los que se divide la firma genuina de un determinado usuario es diferente para cada versión de la firma genuina, lo que hace necesario un método que permita relacionar los trazos de ambas firmas. El método utilizado en el presente trabajo para el emparejamiento automático de trazos es el algoritmo de alineamiento temporal DTW, que se ha descrito en detalle en el capítulo 2 de la presente memoria. El procedimiento llevado a cabo es el siguiente:

1. División en trazos mediante el perfil de velocidad de las dos firmas que se desea emparejar.
2. Cálculo de la distancia entre cada trazo de la primera firma y cada trazo de la segunda firma mediante el algoritmo DTW.
3. Para cada trazo de la primera firma, se selecciona el trazo de la segunda firma cuya distancia DTW es menor (es decir, cuyo *score* calculado mediante la ecuación 2.1 es mayor).

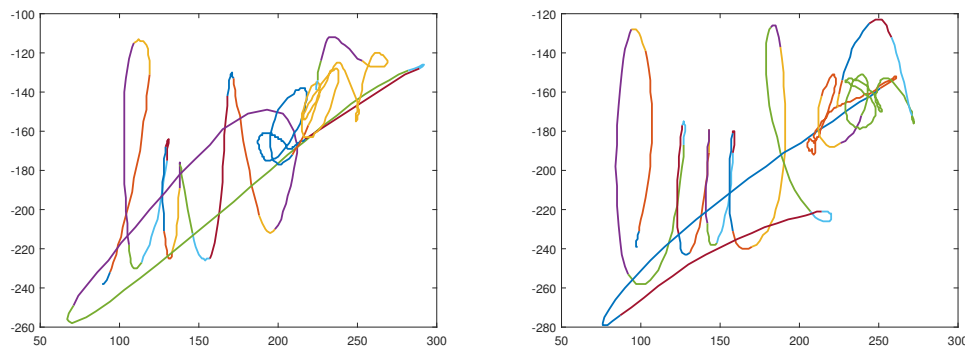


Figura 4.3: Ejemplo de la descomposición en trazos según el perfil de velocidad de dos versiones de la firma genuina de un determinado usuario.

Si se desea reducir el coste computacional de este método de emparejamiento de trazos se puede proceder de la siguiente forma: dado un trazo n de la primera firma (S_n^1), se calcula la distancia únicamente entre dicho trazo y los trazos del S_{n-m}^2 al S_{n+m}^2 de la segunda firma. Este método tiene sentido debido a que la firma manuscrita siempre se realiza en el mismo orden (un usuario inicia y termina su firma siempre por el mismo lugar), de esta forma el trazo n de una firma tendrá una menor distancia habitualmente con el trazo n de la otra firma o con el trazo $n-m$ o $n+m$ siendo m un valor pequeño (por ejemplo, $m = 2$).

4.2.2. Identificación de los trazos más estables de las firmas genuinas de un determinado usuario

Una vez se ha definido un método para el emparejamiento entre trazos de dos firmas genuinas de un determinado usuario (aunque estas hayan sido divididas en distinto número de trazos), es posible estudiar la estabilidad de los trazos de dicha firma. Los trazos más estables de la firma serán aquellos trazos emparejados con los trazos equivalentes de otras versiones de la firma genuina de un usuario independientemente de las pequeñas diferencias que pueda haber entre ellos.

El procedimiento para la identificación de los trazos más estables de la firma genuina de un usuario es el siguiente:

1. Se seleccionan 4 firmas genuinas del usuario que se va a estudiar.
2. Se calculan todas las distancias 1:1 mediante DTW entre las 4 firmas (un total de 6 comparaciones). De las 4 firmas se selecciona la firma cuyas distancias DTW a las demás firmas es menor. A esta firma seleccionada se la conoce como *template*.
3. Se calculan los emparejamientos 1:1 entre los trazos de la firma *template* y los trazos de las 3 firmas restantes.

Se definen dos trazos equivalentes como dos trazos que hacen referencia a una misma región de dos firmas genuinas distintas. En la imagen 4.4 se representan los trazos más estables de la firma de un usuario de la base de datos *eBioSign DS1* sobre las 4 firmas genuinas que se han utilizado para la extracción de dichos trazos estables. La firma que ha sido considerada como *template* se muestra en la imagen superior izquierda.

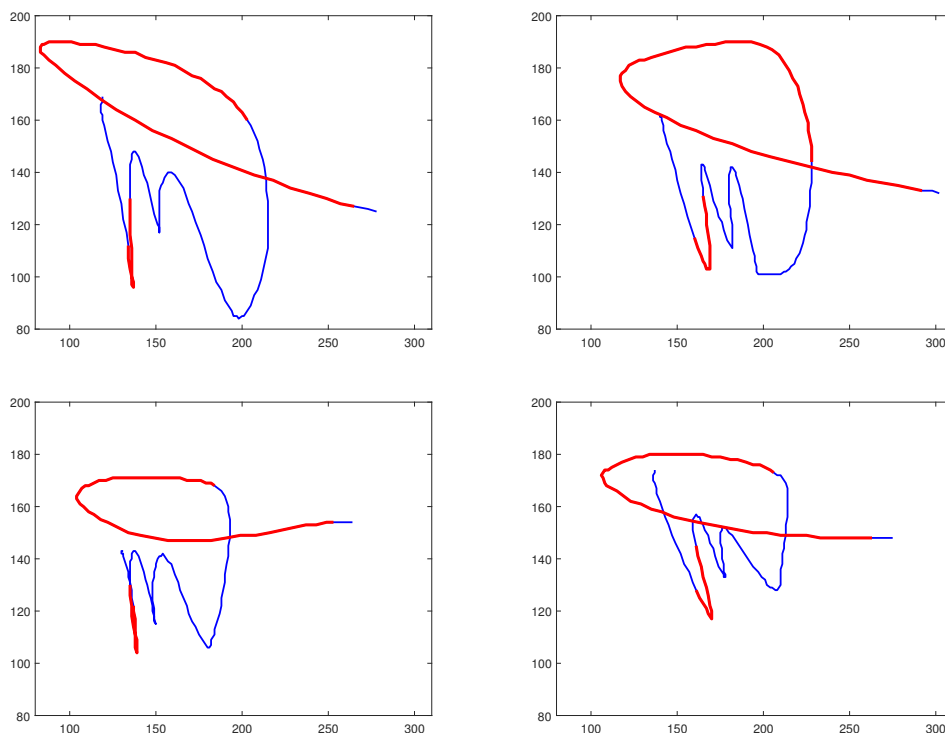


Figura 4.4: En rojo se marcan los trazos más estables de la firma de un usuario, representados sobre 4 de sus firmas genuinas. La imagen superior izquierda representa la firma *template*.

Para verificar que dos trazos son equivalentes se propone la siguiente métrica: se calcula la ubicación del trazo n (UT_n) relativa al tamaño en muestras de la firma a través de la ecuación 4.2, donde m es la muestra central del trazo y N representa el número total de muestras de la firma en cuestión.

$$UT_n = \frac{m}{N} \quad (4.2)$$

Dos trazos, S_n^1 y S_m^2 , de dos firmas diferentes, serán trazos equivalentes si, la UT del trazo S_m^2 es la que más se parece a la UT del trazo S_n^1 . Una vez establecida una medida para determinar equivalencias entre trazos, el procedimiento final para la detección de los trazos más estables de la firma de un usuario es el siguiente:

1. De entre las 4 firmas genuinas de cada usuario, se selecciona la firma *template*: esta es la firma cuyos *scores* en la comparación DTW con todas las demás son más altos (se selecciona esta firma porque, si es la que cuenta con *scores* de las comparaciones más altos, se asume que es la firma que mejor representa la firma genuina del usuario).
2. Para las 4 firmas genuinas, se extraen los trazos según el perfil de velocidad. Utilizando los trazos se calcula el mejor alineamiento entre los trazos de la firma *template* y los trazos de las 3 firmas restantes.
3. Una vez realizado dicho alineamiento, se calculan las UT (mediante la ecuación 4.2) de cada uno de los trazos involucrados en el alineamiento.
4. Para cada uno de los trazos del *template* se calcula la desviación típica del UT de dicho trazo y de los trazos de las 3 firmas genuinas restantes que han sido alineados con el trazo

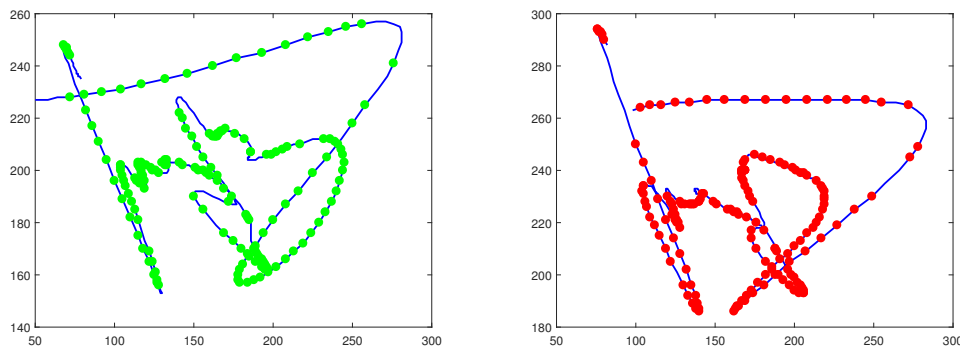


Figura 4.5: *Direct Matching Points* extraídos mediante DTW entre dos firmas genuinas de un usuario de la base de datos *eBioSign DS1*.

del *template*. Si la desviación típica es inferior o igual a 0.05, dicho trazo se tomará como trazo estable (este umbral de desviación típica ha sido seleccionado como el más óptimo tras haberse hecho la prueba con diferentes valores).

4.2.3. Identificación de las muestras más estables de las firmas genuinas de un determinado usuario

En el experimento llevado a cabo en [31] queda demostrada la utilidad del camino óptimo de alineamiento devuelto por el algoritmo DTW como medida para evaluar la estabilidad de una firma. Por otro lado, en [32] los autores introducen el concepto de *Direct Matching Points* (DMPs). Los DMPs son las muestras de una firma que tienen un emparejamiento 1:1 con una única muestra de la segunda firma en el alineamiento de muestras que devuelve el algoritmo DTW.

En este Trabajo de Fin de Máster se ha utilizado una combinación de los anteriores enfoques para encontrar regiones de muestras estables dentro de las firmas genuinas de un usuario.

En la figura 4.5 se muestran a modo de ejemplo los DMPs entre dos firmas genuinas de un usuario de la base de datos *eBioSign DS1*. Tal y como se demuestra en [32], estos DMPs son las muestras más estables de ambas firmas, porque son las muestras que el algoritmo DTW ha sabido emparejar inequívocamente.

Los DMPs varían en función de las dos firmas utilizadas, debido a que las firmas genuinas de un usuario tienen pequeñas variaciones entre ellas. El método propuesto tiene en cuenta estas variaciones a la hora de encontrar las muestras más estables de la firma de un usuario. Los pasos seguidos para encontrar estas muestras son los siguientes:

1. Se seleccionan 4 firmas genuinas del usuario en cuestión.
2. Se calcula la distancia entre todas las firmas y se selecciona la firma cuya distancia es menor con respecto a las 3 firmas restantes. De forma análoga al caso anterior, a la firma seleccionada se la conoce como *template*.
3. Se calculan los DMPs entre la firma *template* y cada una de las otras 3 firmas.
4. Se seleccionan las muestras de la firma *template* que están presentes en los 3 conjuntos de DMPs calculados.

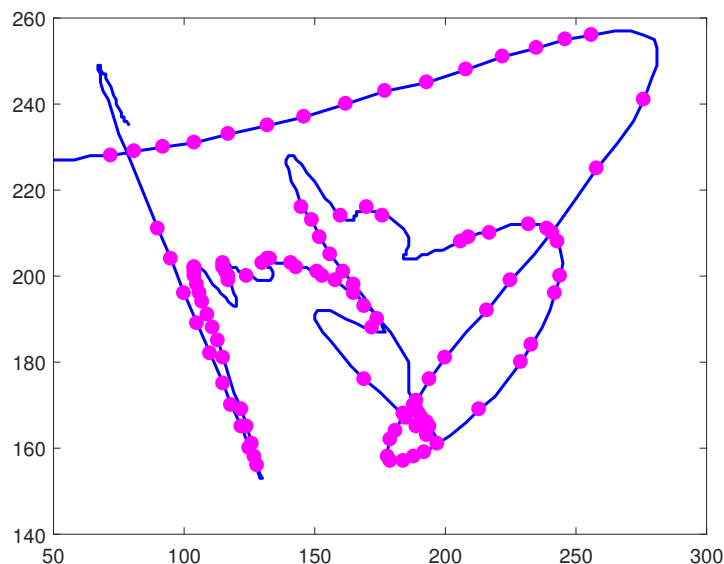


Figura 4.6: Selección de DMPs más estables de 4 firmas genuinas de un usuario de la base de datos *eBioSign DS1*.

	Porcentaje de muestras estables (aprox.)
Trazos estables	78.7 %
Trazos no estables	21.3 %

Tabla 4.1: Distribución de las muestras más estables dentro de los diferentes trazos de una firma.

En la figura 4.6 se muestran la selección de DMPs más estables de 4 firmas genuinas de un usuario de la base de datos *eBioSign DS1*. Una vez se conocen las muestras más estables de una firma y sus trazos (como se ha comentado en el anterior apartado) se puede establecer una relación entre ambos.

4.2.4. Relaciones entre las muestras y trazos más estables de una firma

Una vez se conocen los trazos y las muestras más estables de la firma de un usuario se puede establecer una relación entre ellos, para poder determinar cuáles son las regiones más estables de la firma. En las dos imágenes de la figura 4.7 se muestran los trazos más estables de la firma de un usuario (imagen izquierda) junto con sus muestras más estables (imagen derecha). Se puede apreciar fácilmente como los trazos más estables concentran la gran mayoría de las muestras más estables.

En general, las muestras más estables detectadas en la firma de un usuario, suelen concentrarse dentro de los trazos estables detectados, lo que refuerza la hipótesis de la estabilidad de dichos trazos.

Tras un estudio realizado con 50 usuarios de la base de datos *eBioSign* se ha observado que la distribución de muestras estables entre los trazos de una firma es la mostrada en la tabla 4.1.

Como medida para asegurar que los trazos seleccionados como estables en la firma de un usuario, se ha establecido que al menos el 70 % de las muestras estables detectadas en dicha firma deban coincidir con los trazos más estables. En caso contrario, se concluirá que no se han

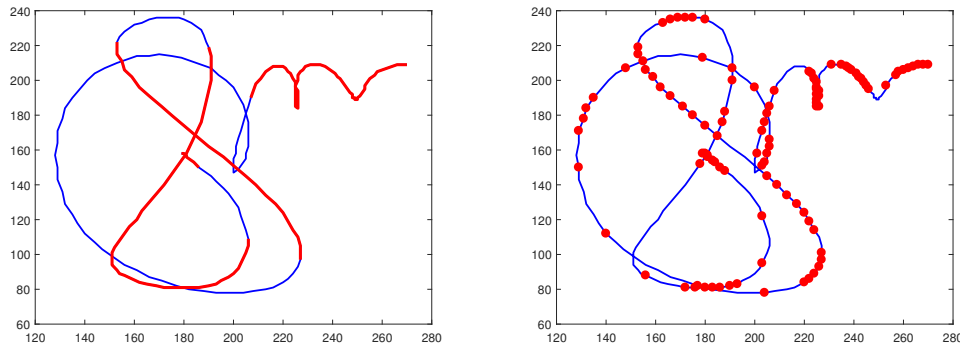


Figura 4.7: En las imágenes superiores se muestran los trazos y muestras más estables de la firma de un usuario de la base de datos *eBioSign* DS1.

conseguido detectar trazos estables en la firma de ese usuario. De entre los 65 y 81 usuarios de los *datasets* de la base de datos *e-BioSign*, DS1 y DS2, únicamente se han encontrado 4 usuarios cuyas firmas no cumplen el umbral del 70 % comentado.

4.3. Métodos alternativos: extracción de trazos mediante el modelo Sigma-Lognormal

El modelo Sigma-Lognormal basado en la Teoría Cinemática de movimientos humanos rápidos permite representar firmas manuscritas dinámicas con un modelo neuromuscular [33].

4.3.1. División de una firma en *lognormal strokes*

En algunos estudios presentes en el estado del arte se ha utilizado el modelo Sigma-Lognormal para generar firmas sintéticas que mejoran el rendimiento de los sistemas de verificación biométrica [34]. En [2] se presenta un enfoque, basado en el modelo Sigma-Lognormal, que permite la descomposición de la firma (S) en N trazos *lognormal*, conocidos como *lognormal strokes* (s_i):

$$S = (s_1, s_2, \dots, s_N) \quad (4.3)$$

Cada uno de estos *lognormal strokes* cuenta con una *lognormal speed*:

$$|\vec{v}_i(t)| = \frac{D_i}{\sqrt{2\pi}\sigma_i(t - t_{0_i})} \exp\left(-\frac{(\ln(t - t_{0_i}) - \mu_i)^2}{2\sigma_i^2}\right) \quad (4.4)$$

con respecto a un tiempo de inicialización (t_{0_i}), la entrada D_i , que corresponde con la distancia cubierta una vez se ha producido el aislamiento, y dos parámetros, μ_i y σ_i relacionados con el retraso *logtime* y el tiempo *logresponse* del sistema neuromuscular que responde a la entrada D_i . La posición angular del movimiento relativo a la dirección de pivote se representa con respecto a un ángulo inicial, θ_{s_i} y un ángulo final θ_{e_i} . Por tanto, cada *lognormal stroke* puede representarse mediante 6 parámetros:

$$s_i = (D_i, t_{0_i}, \mu_i, \sigma_i, \theta_{s_i}, \theta_{e_i}) \quad (4.5)$$

Feature	Description
1	$f_1 = D_i$
2	$f_2 = \mu_i$
3	$f_3 = \sigma_i$
4	$f_4 = \sin(\theta_{s_i})$
5	$f_5 = \cos(\theta_{s_i})$
6	$f_6 = \sin(\theta_{e_i})$
7	$f_7 = \cos(\theta_{e_i})$
8	$f_8 = \Delta t_0 = t_{0_i} - t_{0_{i-1}}$
9	$f_9 = v_2 = \vec{v}_i(t_{2_i}) $
10	$f_{10} = v_3 = \vec{v}_i(t_{3_i}) $
11	$f_{11} = v_4 = \vec{v}_i(t_{4_i}) $
12	$f_{12} = \delta t_{05} = t_{5_i} - t_{0_i}$
13	$f_{13} = \delta t_{15} = t_{5_i} - t_{1_i}$
14	$f_{14} = \delta t_{13} = t_{3_i} - t_{1_i}$
15	$f_{15} = \delta t_{35} = t_{5_i} - t_{3_i}$
16	$f_{16} = \delta t_{24} = t_{4_i} - t_{2_i}$
17	$f_{17} = \Delta t_1 = t_{1_i} - t_{1_{i-1}}$
18	$f_{18} = \Delta t_3 = t_{3_i} - t_{3_{i-1}}$

Tabla 4.2: Conjunto de *stroke features*. Tabla adaptada de [2].

de esta forma, la velocidad observada se reconstruye utilizando las velocidades *lognormal* calculadas para cada trazo:

$$\vec{v}_r(t) = \sum_{i=1}^n \vec{v}_i(t) \quad (4.6)$$

Sin embargo, los autores de [2] no recomiendan utilizar los parámetros de los trazos que se muestran en la ecuación 4.5 sino que recomiendan extraer 18 características (las que se muestran en la tabla 4.2) basadas en estos parámetros y que han demostrado ofrecer un mejor rendimiento.

Las características de la f_9 a la f_{18} se calculan en base a 5 tiempos característicos: t_{1_i}, \dots, t_{5_i} del *lognormal stroke*. Los tiempos $t_{2_i}, t_{3_i}, t_{4_i}$ son los ceros de la primera y segunda derivada de la velocidad calculada en la ecuación 4.4. El tiempo t_{3_i} corresponde con el máximo del *lognormal stroke* (y puede calcularse mediante la ecuación 4.7) y los tiempos t_{2_i} y t_{4_i} corresponden con los puntos de inflexión de la *lognormal*.

$$t_{3_i} = t_{0_i} + \exp(\mu_i - \sigma_i^2) \quad (4.7)$$

Los dos tiempos restantes, t_{1_i} y t_{5_i} se seleccionan para que el intervalo $[t_{1_i}, t_{5_i}]$ contenga el 99.97% del área bajo la curva *lognormal*. Estos tiempos pueden calcularse con las ecuaciones 4.8 y 4.9:

$$t_{1_i} = t_{0_i} + \exp(\mu_i - 3\sigma_i) \quad (4.8)$$

$$t_{5_i} = t_{0_i} + \exp(\mu_i + 3\sigma_i) \quad (4.9)$$

La ubicación de cada uno de los tiempos característicos de una *lognormal* se muestran en la figura 4.8.

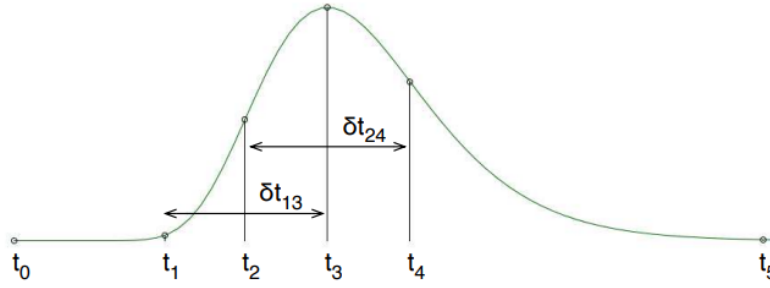


Figura 4.8: Tiempos característicos de una *lognormal*.

4.3.2. Cálculo de la distancia entre dos firmas en base a sus *lognormal strokes*

Los autores de [2] también presentan una medida de distancia ($d(q, r)$) entre una firma $q = (q_1, q_2, \dots, q_N)$ y una firma de referencia $r = (r_1, r_2, \dots, r_M)$, basada en DTW y que puede calcularse mediante la siguiente 4.10:

$$d(q, r) = \min \sum_{i=1}^{|p|} |f_k(q_{p_{i,1}}) - f_k(q_{r_{i,2}})| \quad (4.10)$$

con respecto a cada una de las características f_k , $k \in 1, \dots, 18$, y un camino de alineamiento temporal (p). Utilizando la distancia DTW ($d(q, r)$), se calcula la distancia mínima al conjunto de firmas de referencia R :

$$d_R(q) = \min_{r \in R} d(q, r) \quad (4.11)$$

Por último, se normaliza el valor obtenido mediante la ecuación:

$$\hat{d}_R(q) = \frac{d_R(q)}{\mu_d} \quad (4.12)$$

y donde μ_d se calcula mediante la siguiente fórmula:

$$\mu_d = \frac{1}{|R|} \sum_{i=1}^{|R|} d_{R,r_i}(r_i) \quad (4.13)$$

4.3.3. Explotación de los *lognormal strokes* para mejorar el rendimiento de los sistemas de verificación de firma manuscrita

Resulta complicado establecer relaciones entre los *lognormal strokes* y los trazos de una firma. En el presente Trabajo de Fin de Máster se ha tratado de encontrar cuáles son los *lognormal strokes* que mejor representan una firma, es decir, aquellos más estables, sin embargo, el rendimiento en las comparaciones DTW entre *lognormal strokes* no ha resultado ofrecer un mejor rendimiento que las comparaciones DTW basadas en las 23 *local features* de las firmas.

Sin embargo, pueden encontrarse en la literatura publicaciones que prueban que los *lognormal strokes* permiten caracterizar una firma manuscrita y que ofrecen un excelente rendimiento en

diferentes sistemas [35], lo que invita a pensar que la detección de estabilidad entre los *lognormal strokes* de la firma genuina de un usuario podría mejorar el rendimiento ofrecido por los sistemas de verificación basados en firma manuscrita actuales. El estudio de este aspecto y la posterior incorporación de la estabilidad de los *lognormal strokes* a un sistema de verificación queda pendiente para un trabajo futuro.

5

Experimentos.

En este capítulo se describen los experimentos llevados a cabo para mejorar el rendimiento de los sistemas de verificación basados en firma manuscrita mediante la utilización de técnicas de detección y explotación de los trazos y muestras más estables de la firma de un usuario.

5.1. Introducción

Los experimentos realizados en este capítulo se han llevado a cabo para estudiar los siguientes objetivos:

- Estudiar si la utilización de los trazos y muestras más estables de una firma en la etapa de comparación entre firmas de un sistema de verificación puede mejorar el rendimiento de los sistemas ya existentes.
- Estudiar si los trazos y muestras más estables detectados en la firma de un usuario son robustos frente a diferentes métodos de adquisición de la firma (firmas introducidas mediante *stylus* o firmas introducidas mediante el dedo).

5.2. Bases de datos

Debido a que con los experimentos llevados a cabo en este capítulo se pretende estudiar diferentes situaciones relacionadas con diferentes métodos de adquisición de una firma, se ha seleccionado para ello una base² de datos que cuentan con multitud de firmas que permiten estudiar los mencionados aspectos: *e-BioSign*.

Como se ha comentado en anteriores capítulos de esta memoria, en la actualidad priman las bases de datos de firmas introducidas mediante un dispositivo específico tipo *stylus* por encima de las bases de datos de firmas introducidas mediante el dedo. Adicionalmente, las bases de datos de firma manuscrita no suelen contar con una gran variedad de dispositivos de captura. La principal base de datos que cumple con estas restricciones es **e-BioSign** (que a su vez cuenta con 2 *datasets* distintos: DS1 y DS2).

	Usuarios	Dispositivos	Firmas genuinas por usuario	Falsificaciones por usuario
e-BioSign DS1 (stylus)	65	5	40	30
e-BioSign DS2 (stylus)	81	1	8	6
e-BioSign DS1 (dedo)	65	2	16	12
e-BioSign DS2 (dedo)	81	2	16	12

Tabla 5.1: Detalles de la composición de la base de datos que se ha utilizado para realizar los experimentos descritos en el presente capítulo.

En la tabla 5.1 se ofrecen algunos detalles sobre la composición de la base de datos que se va a utilizar. La utilización de la base de datos *e-BioSign* es de especial interés debido a que cuenta con firmas adquiridas mediante diferentes dispositivos e introducidas tanto mediante *stylus* como mediante el dedo.

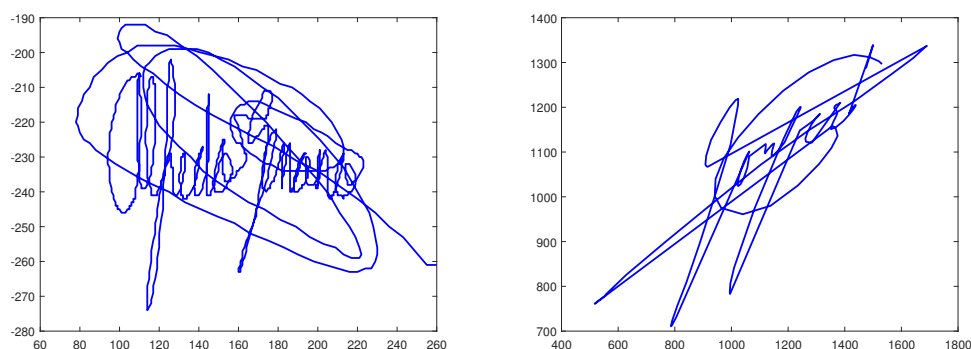


Figura 5.1: Ejemplos de dos firmas genuinas de la base de datos *e-BioSign*.

Aunque no existen diferencias visuales entre las firmas pertenecientes a ambas bases de datos, como puede verse en la figura 5.1, sí existen diferencias en cuanto a la información disponible sobre las firmas.

- La base de datos *e-BioSign*, para las firmas introducidas mediante *stylus* incluye la siguiente información: muestras de las coordenadas espaciales x e y , niveles de presión para cada una de las muestras, marcas de tiempo de cada muestra y trayectorias de los *pen-up*. De toda esta información este trabajo únicamente ha utilizado las muestras de las coordenadas espaciales y los niveles de presión.
- La base de datos *e-BioSign*, para las firmas introducidas mediante dedo incluye la siguiente información: muestras de las coordenadas espaciales x e y y marcas de tiempo para cada una de las muestras. De esta información únicamente se ha trabajado con las muestras de las coordenadas espaciales.

En la sección correspondiente a cada uno de los experimentos llevados a cabo se aportan más detalles relacionados con los usuarios y firmas utilizados en cada experimento.

5.3. Estabilidad de trazos como herramienta para la detección de falsificaciones

Este primer grupo de experimentos se ha llevado a cabo para probar que el análisis y la explotación de trazos estables de la firma genuina de un usuario mejora el rendimiento de los sistemas de verificación de firma manuscrita actuales.

Adicionalmente se han probado otros aspectos, que se describirán más adelante, como diferentes conjuntos de *local features* para realizar las comparaciones entre firmas, si el tamaño de los trazos en los que se dividen las firmas tiene un impacto en el rendimiento final del sistema o si el número de trazos en los que se divide una firma puede dar indicios sobre una potencial falsificación.

5.3.1. Protocolo experimental

Para el experimento principal (grupo de experimentos 1) se ha seleccionado el conjunto de firmas de evaluación de la base de datos *e-BioSign* DS2 [19]. Para el resto de experimentos llevados a cabo se han seleccionado manualmente diferentes conjuntos de firmas en base al comportamiento que se quería estudiar. Los conjuntos de firmas seleccionados se detallan en cada caso concreto.

Para todos los experimentos realizados se han seleccionado, de cada usuario, firmas introducidas mediante *stylus*. En concreto, se han utilizado 8 firmas genuinas y 6 falsificaciones.

Con las firmas seleccionadas se realizan las siguientes fases:

Fase de selección de los trazos más estables de cada usuario

De entre las 8 firmas genuinas de cada usuario, se seleccionan las 4 firmas adquiridas durante la primera sesión de captura y, con ellas, se selecciona la firma *template*: como se comentó en el apartado 4.2.2., esta es la firma cuyos *scores* en la comparación DTW con todas las demás son más altos (se selecciona esta firma porque, si es la que cuenta con *scores* de las comparaciones más altos, se entiende que es la firma que mejor representa la firma genuina del usuario).

Tanto para las 8 firmas genuinas, como para las 6 falsificaciones, se extraen los trazos según el perfil de velocidad. Utilizando los trazos de las 4 firmas genuinas de la primera sesión de captura se calcula el mejor alineamiento entre los trazos de la firma *template* y los trazos de las 3 firmas restantes.

Una vez realizado dicho alineamiento, se calculan las UT (mediante la ecuación 4.2) de cada uno de los trazos involucrados en el alineamiento. Para cada uno de los trazos del *template* se calcula la desviación típica del UT de dicho trazo y de los trazos de las 3 firmas genuinas restantes que han sido alineados con el trazo del *template*. Si la desviación típica es inferior o igual a 0.05, dicho trazo se tomará como trazo estable (este umbral de desviación típica ha sido seleccionado como el más óptimo tras haberse hecho la prueba con diferentes valores).

Fase de explotación de los trazos más estables de cada usuario

Una vez se conocen los trazos más estables de la firma genuina de un usuario, se procede al cálculo de los *scores* de las comparaciones. Por un lado se calculan los *scores* de las comparaciones entre firmas genuinas (comparaciones genuinas) y entre firmas genuinas y falsificaciones

(comparaciones impostoras), pero sin tener en cuenta los trazos estables (este resultado se tomará como referencia). Por otro lado, se calculan los *scores* de las comparaciones genuinas e impostoras, pero teniendo en cuenta únicamente los trazos estables de la firma.

Para el caso de las comparaciones genuinas, se comparan cada una de las 4 firmas de la primera sesión de captura con cada una de las 4 firmas de la segunda sesión de captura (en total, 16 comparaciones). Esto permite tener en cuenta las pequeñas variaciones que sufre una firma con el paso del tiempo. Para el caso de las comparaciones impostoras, se comparan cada una de las 4 firmas de la primera sesión de captura con cada una de las 6 falsificaciones (en total, 24 comparaciones).

El procedimiento para la realización de las comparaciones que tienen en cuenta los trazos estables de la firma que se han seleccionado es el siguiente:

1. De la anterior fase se han almacenado los *UT* de los trazos estables de la firma.
2. Tanto para las comparaciones genuinas, como para las comparaciones impostoras, se seleccionan los trazos cuyo *UT* sea más próximo al *UT* de cada trazo estable.
3. Se calcula el *score* de las comparaciones, pero utilizando los trazos seleccionados.

5.3.2. Sistema de referencia

Como medida de referencia para estudiar si la utilización de los trazos más estables de una firma mejoran el rendimiento de los sistemas de verificación se utiliza el rendimiento obtenido por las comparaciones entre firmas, sin tener en cuenta los trazos estables, únicamente la totalidad de muestras de las firmas.

Para realizar comparaciones entre firmas es frecuente encontrar en la literatura estudios en los que se utilizan únicamente las 2 *local features* correspondientes a las coordenadas espaciales x e y o un subconjunto formado por las siguientes 6 *local features*: las coordenadas espaciales x e y , y la primera y segunda derivadas de ambas coordenadas [36].

La gran mayoría de los experimentos llevados a cabo en el presente trabajo se han realizado con el subconjunto de *local features* formado únicamente por las coordenadas espaciales. La elección de este subconjunto de *local features* está motivado por el hecho de que son las coordenadas espaciales las que se capturan durante el proceso de adquisición de la firma, y es con ellas con las que se extrae el resto de las *local features*, por lo tanto, son muy importantes y cuentan con una gran cantidad de información sobre la firma, por lo que la utilización de dicho subconjunto ofrece buenos resultados. Sin embargo, se han realizado experimentos adicionales donde se utilizan otros conjuntos de *local features* ampliamente utilizados en la literatura para poder establecer comparaciones entre el rendimiento del sistema propuesto y el rendimiento obtenido por otros estudios del estado del arte. En concreto, se ha utilizado el mismo conjunto de *local features* utilizado en [21].

5.3.3. Resultados

A continuación se describen los resultados obtenidos para cada uno de los experimentos llevados a cabo para probar que la estabilidad de trazos permite mejorar el rendimiento de los sistemas de verificación de firma manuscrita.

	Rendimiento (EER)
Sistema con comparaciones que no tienen en cuenta los trazos más estables	25.31 %
Sistema con comparaciones que sí tienen en cuenta los trazos más estables	25.62 %

Tabla 5.2: Rendimiento en términos de EER obtenido por el sistema de verificación que no utiliza los trazos más estables de la firma y por el sistema de verificación que sí utiliza los trazos más estables de la firma.

Experimento 1: Estudio del rendimiento en las comparaciones genuinas e impostoras que tienen en cuenta la estabilidad de trazos

Como se ha comentado en el apartado 5.3.1., para la realización de este experimento se han seleccionado todos los usuarios de la partición de evaluación de la base de datos *e-BioSign* DS2 [19].

En la tabla 5.2 se muestra el rendimiento en términos de EER obtenido por el sistema de verificación que no utiliza los trazos más estables de la firma y por el sistema de verificación que utiliza los trazos más estables de la firma. Como se puede ver en la tabla, ambos rendimientos son similares, sin embargo, si hacemos un análisis más exhaustivo se pueden extraer diferentes conclusiones: si dividimos el espectro de EER en 5 conjuntos: EERs que van de 0 % a 12 %, EERs que van de 12 % a 24 %, EERs que van de 24 % a 36 %, EERs que van de 36 % a 48 % y EERs que van de 48 % a 100 %, observamos que en cada conjunto de EERs ocurre una cosa diferente, y pueden extraerse las siguientes conclusiones:

- Cuando el EER obtenido por el sistema que no tiene en cuenta los trazos estables es bajo (está en el intervalo entre el 0 % y el 24 %), el EER obtenido por el sistema que sí tiene en cuenta los trazos estables es mucho peor.
- Cuando el EER obtenido por el sistema que no tiene en cuenta los trazos estables es alto (es superior al 24 %), el EER obtenido por el sistema que sí tiene en cuenta los trazos estables es mucho mejor.

En la figura 5.2 se muestra la siguiente información: cada par de barras azul y roja representa los EERs promedio (y mediante una barra negra el EER máximo y mínimo) representa uno de los intervalos en los que se ha dividido el EER (la primera barra azul representa el intervalo que va de 0 % a 12 %, la segunda el intervalo que va de 12 % a 24 %, etc.) obtenido por el sistema que no tiene en cuenta los trazos más estables. Cada barra roja representa el EER promedio obtenido por el sistema que sí tiene en cuenta los trazos estables para las firmas que han obtenido un EER en el intervalo representado por la barra azul de la izquierda.

La conclusión que puede extraerse de este análisis es que, cuando el EER obtenido en una comparación DTW entre dos firmas es bajo, la utilización de los trazos más estables de las firmas no ofrecerá un mejor rendimiento, sin embargo, cuando el EER obtenido en la comparación DTW es alto, la utilización de los trazos más estables mejorará dicho rendimiento. Este hecho permite implementar un sistema que no utilice los trazos estables mientras el error obtenido esté por debajo de un umbral y que utilice los trazos estables de las firmas si el error supera dicho umbral.

Si repetimos los experimentos realizados en este apartado, pero utilizando el conjunto de *local features* óptimo, que se utilizó en [21], obtenemos los resultados que se muestran en la tabla 5.3. En este caso, la distribución de EERs es mucho más baja, ya que el conjunto de *local features*

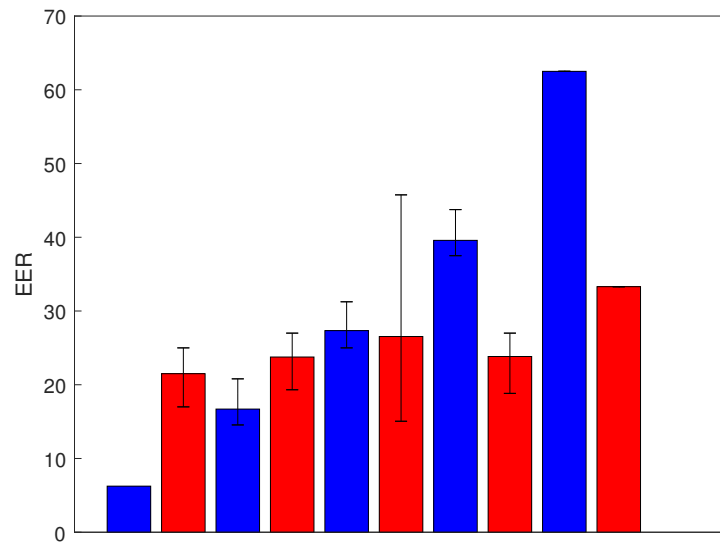


Figura 5.2: División en intervalos del EER obtenido. Las barras azules representan el EER promedio de cada intervalo (EERs que van de 0 % a 12 %, EERs que van de 12 % a 24 %, EERs que van de 24 % a 36 %, EERs que van de 36 % a 48 % y EERs que van de 48 % a 100 %) obtenido por el sistema que no tiene en cuenta los trazos estables. Las barras rojas representan el EER promedio obtenido por el sistema que sí tiene en cuenta los trazos estables, para los usuarios que obtuvieron un EER dentro del intervalo de la barra azul de su izquierda cuando se calcularon las comparaciones DTW sin tener en cuenta los trazos estables.

	Rendimiento (EER)
Sistema con comparaciones que no tienen en cuenta los trazos más estables	11.07 %
Sistema con comparaciones que sí tienen en cuenta los trazos más estables	12.21 %

Tabla 5.3: Rendimiento en términos de EER obtenido por el sistema de verificación que no utiliza los trazos más estables de la firma y por el sistema de verificación que sí utiliza los trazos más estables de la firma.

utilizado ha demostrado en el pasado ser el que mejor resultados ofrece en la comparación entre firmas. Sin embargo, se observa un comportamiento similar al mostrado en la figura 5.2, pero en este caso se muestra en la figura 5.3: en los usuarios que obtienen EERs bajos cuando se realizan comparaciones DTW entre sus firmas, la utilización de trazos estables no resulta ser efectiva, sin embargo, en los usuarios con EERs más altos, la utilización de los trazos más estables produce mejores resultados. Cabe destacar que en este caso, los EERs han sido en general más bajos, debido a que se ha utilizado el subconjunto de *local features* presentado en [21], que ha demostrado ofrecer mejores resultados en la verificación de firma manuscrita dinámica.

Experimento 2: Estudio del impacto del tamaño de los trazos en el rendimiento del sistema

A lo largo de este trabajo se ha detectado que una de las variables críticas para la implementación de un sistema de verificación basado en la estabilidad de trazos es el tamaño de dichos trazos.

Como se comentó en el capítulo 4 de la presente memoria, el algoritmo de división de una firma en trazos según su perfil de velocidad permite generar **trazos grandes** (divide la firma en trazos según estos tengan una velocidad superior o inferior a la media), **trazos medianos** (divide la firma en trazos según estos tengan una velocidad superior a la media más la desviación típica, inferior a la media menos la desviación típica o en el intervalo entre la media más la desviación típica y la media menos la desviación típica) y **trazos pequeños** (divide la firma en trazos según estos tengan una velocidad superior a la media más la desviación típica, inferior a la media menos la desviación típica, pero superior que la media o superior a la media menos la desviación típica, pero inferior que la media).

En la figura 5.4 se muestra la evolución de los *scores* de una serie de comparaciones entre las firmas de 3 usuarios. Sobre el eje x se muestran diferentes comparaciones llevadas a cabo (las comparaciones de la 1 a la 3 son comparaciones genuinas entre la firma *template* y las 3 firmas genuinas restantes. La comparación 4 es una comparación entre 2 firmas genuinas (pero ninguna de ellas es la firma *template*). Las comparaciones de la 5 a la 7 son comparaciones impostoras entre la firma *template* y 3 falsificaciones. La comparación 8 es una comparación aleatoria entre la firma *template* y la firma genuina de otro usuario de la base de datos). Comportamientos similares al mostrado en la figura se pueden observar para otros usuarios de la base de datos.

En la figura 5.4 pueden observarse los siguientes aspectos:

- Por un lado, los *scores* de las **comparaciones genuinas** obtenidos por la utilización de **trazos grandes** (representados por las líneas rojas) de la firma muestran, en general, un comportamiento más parecido a los *scores* obtenidos en las comparaciones sin trazos. Los trazos medianos (representados por las líneas verdes) y pequeños (representados por las

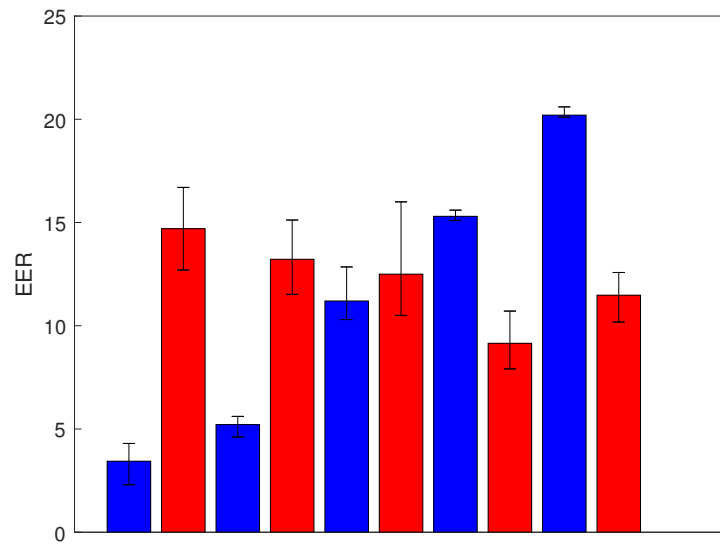


Figura 5.3: División en intervalos del EER obtenido. Las barras azules representan el EER promedio de cada intervalo (EERs que van de 0 % a 5 %, EERs que van de 5 % a 10 %, EERs que van de 10 % a 15 %, EERs que van de 15 % a 20 % y EERs que van de 20 % a 25 %) obtenido por el sistema que no tiene en cuenta los trazos estables. Las barras rojas representan el EER promedio obtenido por el sistema que sí tiene en cuenta los trazos estables, para los usuarios que obtuvieron un EER dentro del intervalo de la barra azul de su izquierda cuando se calcularon las comparaciones DTW sin tener en cuenta los trazos estables.

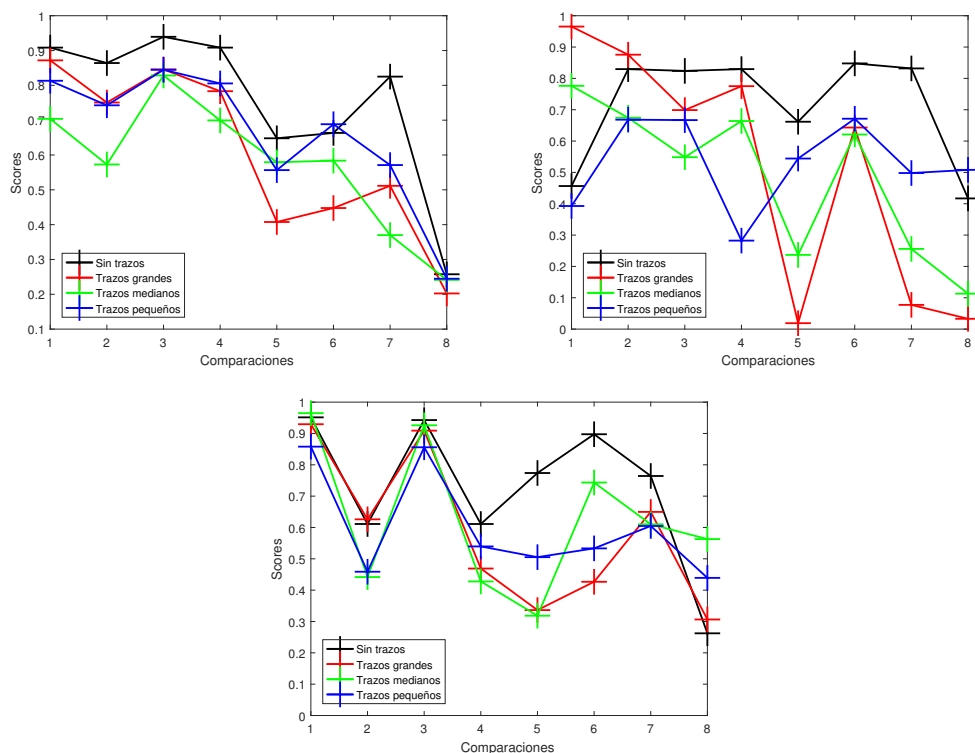


Figura 5.4: Evolución de los *scores* en función del tamaño de los trazos utilizados en las comparaciones para 3 usuarios diferentes (cada gráfica corresponde con un usuario distinto).

líneas azules) degradan un poco más el rendimiento del sistema, aunque las diferencias en este caso no son muy notables.

- Por otro lado, los *scores* de las **comparaciones impostoras** obtenidos por la utilización de **trazos grandes** son significativamente menores que los obtenidos con los trazos medianos y pequeños, lo que implica que el sistema ha reconocido con un mejor margen que una de las firmas que se está comparando no es genuina.
- Con todos los tamaños de trazos puede observarse que, en general, para el caso de las comparaciones genuinas los *scores* se reducen muy poco (en algunos casos llegan a aumentar) con respecto a los *scores* obtenidos en comparaciones sin tener en cuenta trazos, mientras que los *scores* para el caso de las comparaciones impostoras se reducen en una mayor medida.

Podemos concluir por tanto que la utilización de divisiones de las firmas en trazos grandes obtiene un rendimiento mayor en las comparaciones.

Experimento 3: Estudio de la distribución del número de trazos en firmas genuinas y falsificaciones

Durante la realización de este trabajo se ha observado que, en general, el número de trazos en los que se divide una firma es superior para el caso de las falsificaciones que para el caso de firmas genuinas.

En la figura 5.5 puede observarse el promedio de número de trazos en los que se divide una firma genuina (la barra izquierda de cada color) y una falsificación (la barra derecha de cada

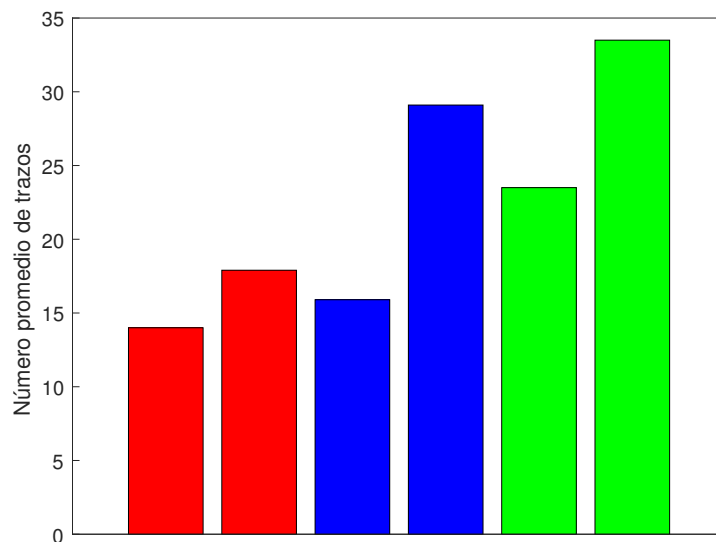


Figura 5.5: Promedio del número de trazos en los que se divide una firma genuina (de cada color, la barra izquierda) y una falsificación (de cada color, la barra derecha). El color rojo representa la división de la firma en trazos grandes, el azul, en trazos medianos y el verde, en trazos pequeños.

color). Estos promedios han sido calculados con todos los usuarios de la base de datos *e-BioSign*:

- Para el caso de división en **trazos grandes**, el número promedio de trazos en los que se divide una falsificación es un **27.85 % mayor** que el número promedio de trazos en los que se divide una firma genuina.
- Para el caso de división en **trazos medianos**, el número promedio de trazos en los que se divide una falsificación es un **83.02 % mayor** que el número promedio de trazos en los que se divide una firma genuina.
- Para el caso de división en **trazos pequeños**, el número promedio de trazos en los que se divide una falsificación es un **42.55 % mayor** que el número promedio de trazos en los que se divide una firma genuina.

Con estos datos se puede extraer la conclusión de que el hecho de que una firma resulte ser dividida en un número significativamente mayor que el promedio de las firmas genuinas puede ser un indicio de que dicha firma es una falsificación.

Experimento 4: Estudio del impacto de la complejidad de la firma en la división en trazos en base al perfil de velocidad

Numerosos trabajos de la literatura han estudiado el impacto de la complejidad de una firma en el rendimiento de un sistema biométrico de verificación [37] [38] [39]. Algunos autores describen la complejidad de una firma como la cantidad de información que hay en ella (un concepto muy relacionado con la entropía), mientras que otros utilizan un enfoque más simple, basado en el número de trazos de la firma y en el número de cruces entre ellos. En general:

- Se considera una firma como de **baja complejidad** si cuenta con pocos trazos y estos tienen pocos cruces entre ellos. Un ejemplo de firma de baja complejidad puede observarse en la imagen izquierda de la figura 5.6.
- Se considera una firma como de **alta complejidad** si cuenta con muchos trazos y estos tienen muchos cruces entre ellos. Un ejemplo de firma de alta complejidad puede observarse en la imagen derecha de la figura 5.6.

En el caso de las firmas de baja complejidad, debido a que el usuario ha realizado pocos trazos a la hora de dibujar la firma, la extracción de trazos mediante el perfil de velocidad divide la firma en pocos trazos. En el caso de las firmas de alta complejidad ocurre lo contrario. En concreto, para el caso de la firma mostrada en la imagen izquierda de la figura 5.6, la división se ha realizado en 10 trazos, mientras que para el caso de la firma mostrada en la imagen derecha, la división se ha realizado en 36 trazos.

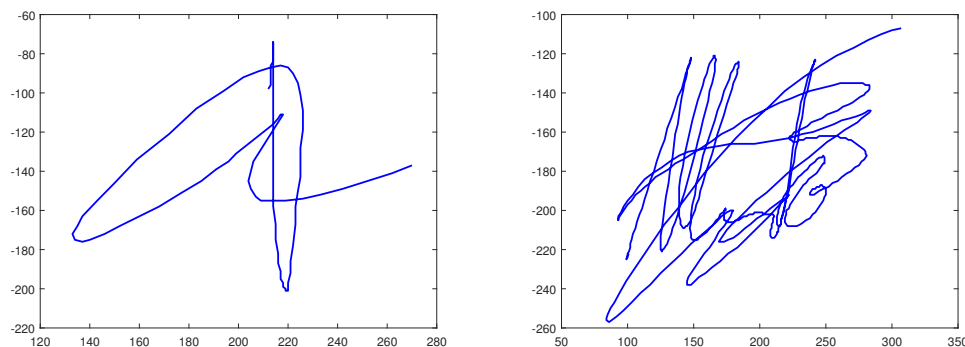


Figura 5.6: Ejemplos de 2 firmas de diferente complejidad de la base de datos *e-BioSign DS2*: baja complejidad (imagen izquierda) y alta complejidad (imagen derecha).

En la figura 5.7 se muestra la evolución de los *scores* para las mismas 8 comparaciones realizadas en la figura 5.4, pero en este caso las comparaciones se han realizado con los usuarios de las firmas de la figura 5.6, tanto para el caso de comparaciones realizadas sin tener en cuenta los trazos más estables como para el caso de comparaciones teniendo en cuenta los trazos más estables de la firma. Puede observarse como para el caso de la firma de alta complejidad (imagen derecha) el rendimiento mejora sustancialmente: los *scores* de las comparaciones que tienen en cuenta los trazos más estables son bastante menores que los *scores* de las comparaciones que no tienen en cuenta los trazos, en el caso de las comparaciones impostoras, mientras que en el caso de las comparaciones genuinas los *scores* son relativamente similares. Esto no ocurre para el caso de la firma de baja complejidad (imagen izquierda), donde se puede observar que tanto los *scores* de las comparaciones que tienen en cuenta los trazos como los de las que no, son bastante similares.

Resultados similares a los aquí descritos pueden observarse en otras firmas de baja y alta complejidad. La conclusión que puede extraerse de este análisis es la siguiente: en las firmas de baja complejidad, fácilmente falsificables, es difícil encontrar trazos estables que caractericen bien a la firma y permitan discernir entre una firma genuina y una falsificación, mientras que en las firmas de alta complejidad es posible encontrar trazos estables en las firmas genuinas que faciliten la detección de falsificaciones.

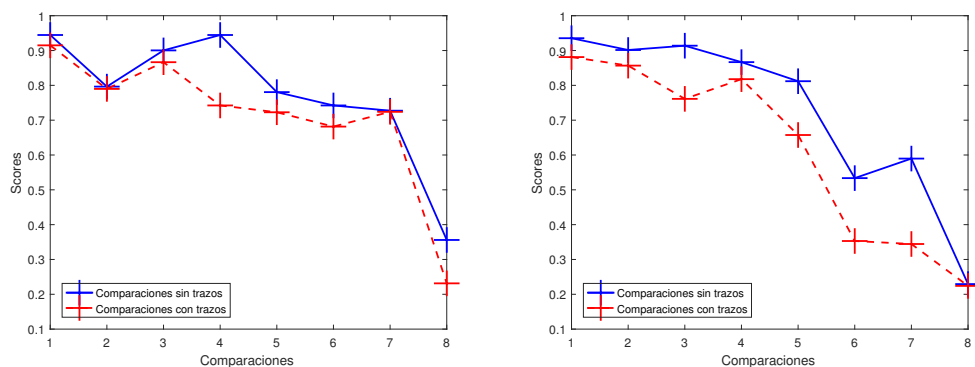


Figura 5.7: Evolución de los *scores* en diferentes comparaciones. A la izquierda se muestra la evolución para las comparaciones realizadas con la firma de baja complejidad de la figura 5.6 y a la derecha se muestra la evolución para las comparaciones realizadas con la firma de alta complejidad.

5.4. Estabilidad de trazos entre firmas introducidas mediante *stylus* y dedo

En el anterior apartado se ha demostrado como la detección y explotación de los trazos más estables de la firma genuina de un usuario permiten mejorar la detección de falsificaciones y el rendimiento de los sistemas de verificación en algunas situaciones: cuando el error obtenido por el sistema que no tiene en cuenta los trazos estables es demasiado alto. En el presente apartado se va a estudiar si los trazos estables detectados en las firmas genuinas de un usuario introducidas mediante *stylus* ofrecen el mismo rendimiento en las firmas introducidas mediante el dedo.

5.4.1. Protocolo experimental

El protocolo experimental llevado a cabo en este grupo de experimentos es similar al utilizado en el anterior caso, pero se ha adaptado para realizar el estudio de la estabilidad de las firmas introducidas mediante el dedo:

- Utilizando 4 firmas genuinas de un usuario, introducidas mediante *stylus*, se extrae la firma *template* y se seleccionan los trazos más estables.
- Se seleccionan 4 firmas genuinas y 3 falsificaciones del mismo usuario, pero que en este caso hayan sido introducidas mediante el dedo.
- Se calculan los *scores* de las comparaciones entre las firmas genuinas y entre las firmas genuinas y las falsificaciones, utilizando los trazos más estables ya detectados y sin utilizarlos, de forma que se pueda estudiar el impacto de la utilización de los mismos.

5.4.2. Resultados

En la imagen 5.8 se muestra una firma genuina introducida mediante *stylus* (imagen izquierda) y mediante dedo (imagen derecha) de un determinado usuario de la base de datos *e-BioSign DS2*. Aunque ambas son firmas genuinas del mismo usuario, existen diferencias notables entre ellas. En general, las diferencias existentes entre versiones de la firma genuina de un usuario que han sido introducidas usando métodos diferentes son las siguientes:

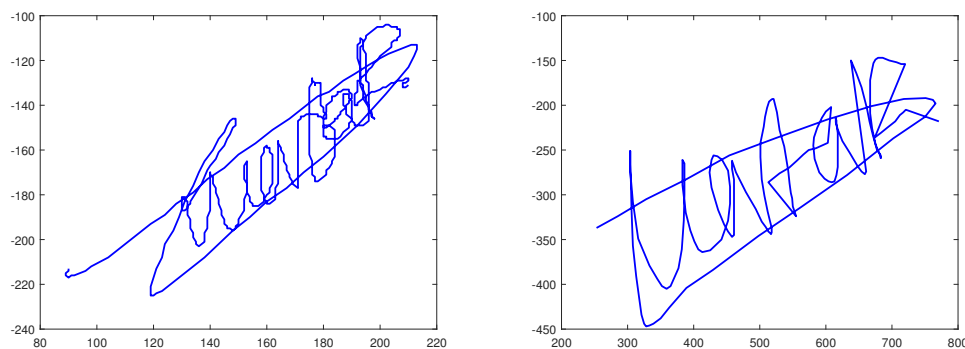


Figura 5.8: Ejemplos de una firma genuina introducida mediante *stylus* (imagen izquierda) y mediante dedo (imagen derecha) de un determinado usuario de la base de datos *e-BioSign DS2*.

Tipo de comparaciones	Reducción media <i>scores stylus</i>	Reducción media <i>scores dedo</i>
Comparaciones genuinas	0.0509	0.1142
Comparaciones impostoras	0.2618	0.1213
Comparaciones aleatorias	0.0819	0.0878

Tabla 5.4: Reducción media de los *scores* en comparaciones genuinas, impostoras y aleatorias, para el caso de firmas introducidas mediante *stylus* y mediante el dedo.

- La fina punta del *stylus* permite realizar un nivel de detalle en las firmas superior al que es posible realizar con el dedo, cuya superficie de contacto con la pantalla del dispositivo de captura es mucho mayor.
- Las firmas realizadas mediante el dedo cuentan habitualmente con curvaturas, lazos y cambios de trazo más bruscos (por ejemplo, los giros y lazos de las firmas suelen tener esquinas y picos, mientras que las mismas firmas, pero introducidas mediante *stylus* cuentan con giros y lazos con esquinas mucho más redondeadas). En general, las transiciones entre trazos en las firmas introducidas mediante *stylus* son mucho más suaves.

Estas diferencias degradan el rendimiento del sistema, como ha quedado demostrado en diferentes publicaciones de la literatura [12] [11] [4], lo que hace que la línea de investigación que busca adaptar los sistemas de verificación de firma manuscrita desarrollados para *stylus* a las firmas introducidas mediante el dedo esté ganando cada vez más relevancia dentro del estado del arte.

Experimento 6: Estudio del impacto de los trazos estables detectados en firmas genuinas introducidas mediante *stylus* sobre las comparaciones realizadas con firmas del mismo usuario introducidas mediante el dedo

En la tabla 5.4 se muestra la reducción media de los *scores* en comparaciones genuinas, impostoras y aleatorias. Se observa que, mientras que para el caso de los *scores* obtenidos con firmas introducidas mediante *stylus* la reducción media de los *scores* de las comparaciones genuinas es mucho menor que la reducción media de los *scores* de las comparaciones impostoras

y aleatorias, esto no se cumple con los *scores* obtenidos en las comparaciones que involucran firmas introducidas mediante el dedo.

Con los datos mostrados en la tabla 5.4 puede concluirse que los trazos estables extraídos mediante las firmas genuinas introducidas mediante *stylus* de un determinado usuario no mejoran el rendimiento en las comparaciones entre firmas del mismo usuario introducidas mediante el dedo que tienen en cuenta los mencionados trazos estables.

Experimento 7: Estudio de los trazos estables de la firma genuina de un usuario introducida mediante el dedo

En el anterior grupo de experimentos ha quedado demostrado que la utilización de los trazos estables detectados en las firmas genuinas introducidas mediante *stylus* no ofrecen buenos resultados en las comparaciones realizadas entre firmas del mismo usuario introducidas mediante el dedo.

Este conjunto de experimentos busca estudiar el impacto que tienen sobre las comparaciones entre firmas de un usuario introducidas mediante el dedo la utilización de los trazos estables detectados en las firmas genuinas de dicho usuario introducidas mediante el dedo.

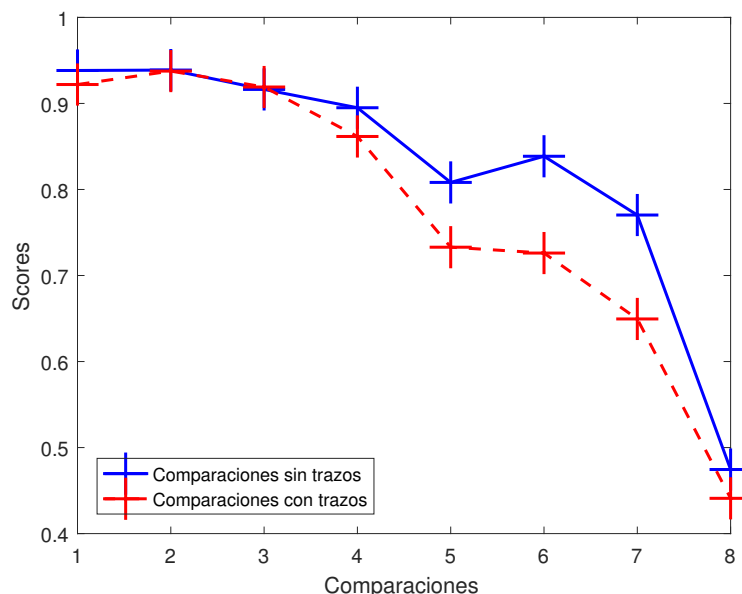


Figura 5.9: Evolución promedio de los *scores* en comparaciones genuinas, impostoras y aleatorias en usuarios con firmas introducidas mediante el dedo.

En la figura 5.9 se muestra la evolución promedio de los *scores* en comparaciones genuinas (comparaciones 1 a la 4), impostoras (comparaciones 5 a la 7) y aleatorias (comparación 8) en usuarios con firmas introducidas mediante el dedo (los usuarios seleccionados para este experimento han sido los usuarios cuyas firmas son más complejas). Cada comparación ha sido realizada siguiendo el mismo protocolo que en la figura 5.4. Puede observarse que la reducción en los *scores* de las comparaciones genuinas es significativamente menor que la reducción en los *scores* de las comparaciones impostoras, de lo que podemos concluir que, al igual que ocurría con el caso de los trazos estables detectados en firmas genuinas introducidas mediante *stylus*, en el caso de los trazos estables detectados en firmas genuinas introducidas mediante el dedo, el rendimiento de las comparaciones aumenta, pero, de nuevo, esto ocurre únicamente con un grupo de usuarios (aquellos con errores más altos cuando no se tienen en cuenta los trazos estables).

Experimento 8: Estudio de la distribución del número de trazos en firmas genuinas y falsificaciones introducidas mediante el dedo

En el grupo de experimentos 3 quedó demostrado como el número de trazos en los que se dividen las falsificaciones es mayor que el número de trazos en los que se dividen las firmas genuinas. En la figura 5.10 se muestra en las barras azules el número promedio de trazos en los que se divide una firma genuina introducida mediante el dedo (barra izquierda) y el número promedio de trazos en los que se divide una falsificación introducida mediante el dedo (barra derecha). En rojo se muestra el análogo, pero para el caso de firmas de los mismos usuarios introducidas mediante *stylus*. Cabe destacar que para este grupo de experimentos se ha seleccionado manualmente un conjunto de firmas de una complejidad media y alta, dado que este comportamiento no es del todo visible en firmas de complejidad baja que cuentan con muy pocos trazos.

Podemos ver en la figura como, tanto para el caso de las firmas genuinas, como para el caso de las falsificaciones, el número de trazos en el que se dividen las firmas introducidas con el dedo es sensiblemente menor. Este hecho era esperable debido a que, como se ha comentado al inicio del apartado 5.4.3., en general, las firmas introducidas mediante el dedo cuentan con trazos con menor detalle (las firmas introducidas con el dedo están muy condicionadas al hecho de que la superficie del dedo apoyada sobre la pantalla del dispositivo de captura es mucho mayor que la superficie de la fina punta del *stylus*, lo que hace que los trazos introducidos mediante el dedo sean más sencillos) y más sencillos, lo que hace que la extracción de trazos mediante el perfil de velocidad también particione la firmas en un menor número de trazos.

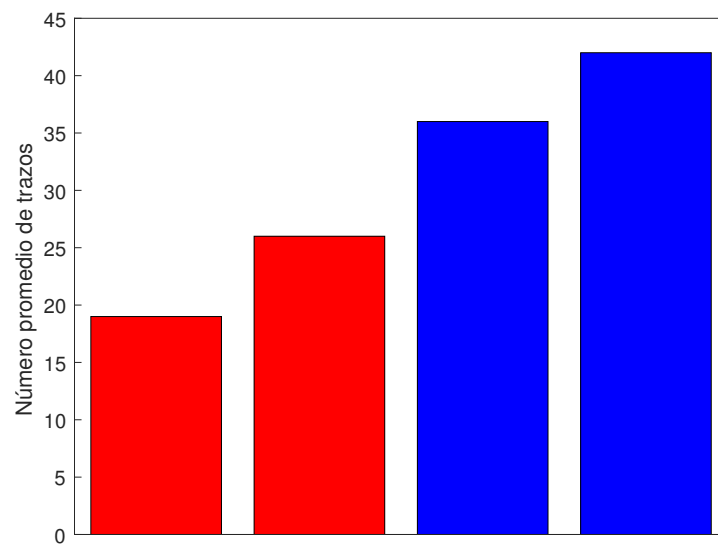


Figura 5.10: Número promedio de trazos en los que se divide las firmas introducidas mediante el dedo (barras rojas) y mediante *stylus* (barras azules) de un grupo de usuarios. De cada color, la barra izquierda representa las firmas genuinas del usuario y la barra derecha representa sus falsificaciones.

5.5. Evaluación de las falsificaciones generadas para la base de datos *MobileTouchDB* y estudio del impacto de los trazos más estables en la etapa de verificación

Como se ha comentado en anteriores secciones de la presente memoria, la base de datos *MobileTouchDB* fue capturada en un escenario no controlado (cada usuario podía realizar las falsificaciones en el lugar que deseara) e involucra multitud de dispositivos (algunos de los *smartphone* utilizados son de gama alta, mientras que otros son *smartphone* de una gama más baja). Estas características de *MobileTouchDB*, junto con el hecho de que las falsificaciones generadas se realizaron con mucha información disponible, invita a pensar que el rendimiento de la etapa de verificación de esta base de datos será inferior al rendimiento obtenido con la base de datos *e-BioSign*.

	Rendimiento (EER)
Sistema con comparaciones que no tienen en cuenta los trazos más estables	17.32 %
Sistema con comparaciones que sí tienen en cuenta los trazos más estables	18.15 %

Tabla 5.5: Rendimiento en términos de EER obtenido por el sistema de verificación que no utiliza los trazos más estables de la firma y por el sistema de verificación que sí utiliza los trazos más estables de la firma. Este proceso de verificación se realizó en la base de datos *MobileTouchDB*.

En la tabla 5.5 se muestran los EERs obtenidos en la etapa de verificación sobre todos los usuarios de la base de datos *MobileTouchDB*, tanto por el sistema que no tiene en cuenta los trazos estables detectados en la firma genuina de un usuario, como por el sistema que sí tiene en cuenta dichos trazos. A la vista de los resultados, que han sido obtenidos mediante el subconjunto óptimo de características presentado en [21], podemos concluir como, efectivamente, las falsificaciones realizadas para los usuarios de la base de datos *MobileTouchDB* son de una calidad mayor que las falsificaciones de otras bases de datos del estado del arte.

De nuevo, el EER obtenido por los sistemas que no tienen en cuenta los trazos más estables y que sí que los tienen en cuenta es muy similar. Si hacemos un estudio más exhaustivo de la distribución de EERs y dividimos los usuarios en los siguientes grupos: usuarios con EERs en el intervalo entre 0% y 6%, usuarios con EERs en el intervalo entre 6% y 12%, usuarios con EERs en el intervalo entre 12% y 18%, usuarios con EERs en el intervalo entre 18% y 24% y usuarios con EERs en el intervalo entre 24% y 30% se observan comportamientos similares a los mostrados en las figuras 5.2 y 5.3, tal y como se muestra en la figura 5.11 lo que, de nuevo, confirma que el sistema que utiliza los trazos más estables de la firma es especialmente útil en los usuarios de la base de datos que cuentan con un error mayor.

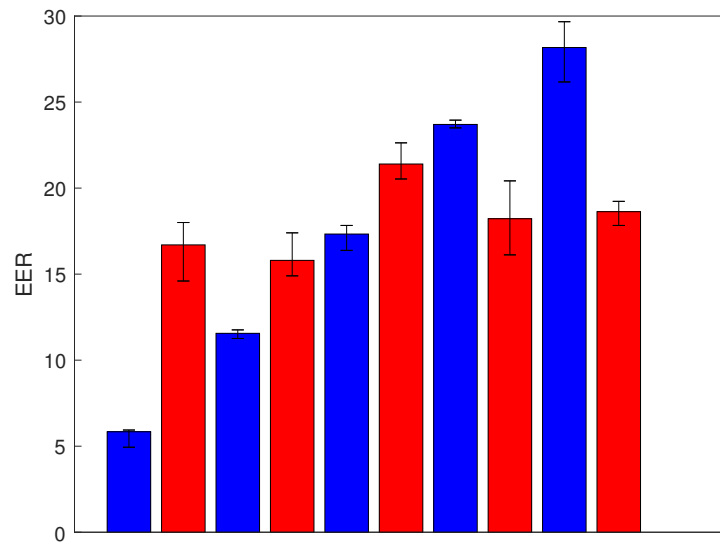


Figura 5.11: División en intervalos del EER obtenido. Las barras azules representan el EER promedio de cada intervalo (EERs que van de 0 % a 6 %, EERs que van de 6 % a 12 %, EERs que van de 12 % a 18 %, EERs que van de 18 % a 24 % y EERs que van de 24 % a 30 %) obtenido por el sistema que no tiene en cuenta los trazos estables. Las barras rojas representan el EER promedio obtenido por el sistema que sí tiene en cuenta los trazos estables, para los usuarios que obtuvieron un EER dentro del intervalo de la barra azul de su izquierda cuando se calcularon las comparaciones DTW sin tener en cuenta los trazos estables.

6

Conclusiones y trabajo futuro

6.1. Conclusiones

El estudio realizado durante este Trabajo de Fin de Máster se ha centrado en la detección de los trazos más estables de la firma genuina de un determinado usuario, para su posterior explotación dentro de un sistema biométrico de verificación de firma manuscrita dinámica.

En primer lugar se ha demostrado que la utilización de los trazos más estables de la firma genuina de un usuario, para la realización de comparaciones DTW entre firmas, ofrece una mejora de rendimiento únicamente en el caso de los usuarios cuyas firmas obtienen un mayor error en las comparaciones DTW que involucran la totalidad de muestras de las firmas. En el caso de los usuarios que obtienen un EER bajo en las comparaciones DTW que involucran todos los trazos de la firma, la utilización únicamente de los trazos estables degrada el rendimiento del sistema. Se ha concluido que los usuarios cuyas firmas son más complejas (involucran un mayor número de trazos y un mayor número de cruces entre ellos) funcionan mejor con la extracción y explotación de sus trazos estables que los usuarios cuyas firmas son más simples (menor número de trazos y menos cruces entre ellos).

En segundo lugar, se ha encontrado que las falsificaciones de una firma manuscrita se dividen, en general, en un mayor número de trazos cuando se ejecuta sobre ellas el algoritmo de extracción de trazos basado en el perfil de velocidad de la firma. Este hecho permite implementar un nuevo módulo dentro de los sistemas de verificación de firma manuscrita dinámica actuales que sospeche que una firma puede ser una falsificación si el número de trazos en los que se ha dividido según el perfil de velocidad es notablemente superior al promedio de número de trazos de otras firmas del usuario.

Por último, se ha probado que los trazos más estables que pueden encontrarse en las firmas genuinas introducidas mediante un útil específico de escritura, como un lápiz tipo *stylus*, de un determinado usuario no coinciden con los trazos más estables que pueden encontrarse en las versiones de la firma genuina de dicho usuario que han sido introducidas mediante el dedo. Que no existan coincidencias significativas entre las trazos estables extraídos de firmas de un mismo usuario introducidas con distintos métodos implica que las diferencias existentes entre estos tipos de firmas (e.g., las firmas introducidas mediante *stylus* cuentan con niveles de detalle más altos y trazos más suavizados que las firmas introducidas mediante el dedo) condicionan la estabilidad de un trazo.

6.2. Trabajo futuro

Durante el estudio desarrollado en este Trabajo de Fin de Máster se han encontrado las siguientes líneas de investigación que pueden dar lugar a un trabajo futuro:

- Estudio de la estabilidad de los *lognormal strokes* de las diferentes versiones de la firma genuina de un determinado usuario para su posterior incorporación dentro de un sistema biométrico de verificación de firma manuscrita dinámica.
- Estudio de otras técnicas de alineamiento temporal dinámico, como aquellas basadas en *deep learning* que puedan sustituir o complementar al algoritmo DTW y estudio del rendimiento obtenido por dichos sistemas cuando se tienen en cuenta los trazos más estables de la firma de un usuario.
- Desarrollo de un nuevo algoritmo de división de una firma manuscrita en trazos, que sea más robusto que el algoritmo basado en el perfil de velocidad de una firma, y que permita establecer conexiones más claras entre trazos equivalentes de distintas versiones de la firma genuina de un determinado usuario.
- Estudio de las falsificaciones generadas para la base de datos *MobileTouchDB*: EERs obtenidos por cada usuario en función del tipo de falsificación, análisis del EER en función de la complejidad de la firma, etc.

Bibliografía

- [1] M. Martinez-Diaz. Dynamic signature verification for portable devices. *TFM. Escuela Politécnica Superior Universidad Autónoma de Madrid*, November 2008.
- [2] A. Fischer and R. Plamondon. A dissimilarity measure for on-line signature verification based on the sigma-lognormal model. *17th Biennial Conference of the International Graphonomics Society*, June 2015.
- [3] J. Gismero. Adquisición y análisis de información manuscrita en entornos móviles. *TFG. Escuela Politécnica Superior, Universidad Autónoma de Madrid*, Junio 2019.
- [4] C. González. Adaptación de sistemas de verificación de firma manuscrita a dispositivos móviles. *TFG. Escuela Politécnica Superior, Universidad Autónoma de Madrid*, 2019.
- [5] Vivian L. Blankers, C. Elisa van den Heuvel, Katrin Franke, and Louis Vuurpijl. Icdar 2009 signature verification competition. In *Proc. ICDAR.*, pages 1403–1407, 2009.
- [6] J. Fierrez-Aguilar, S. Krawczyk, J. Ortega-Garcia, and A. K. Jain. Fusion of local and regional approaches for on-line signature verification. In *Proc. Intl. Workshop on Biometric Recognition Systems, IWBRs*, volume 3781 of *LNCS*, pages 188–196. Springer, October 2005.
- [7] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri. Template protection for hmm-based on-line signature authentication. In *Proc. IEEE Computer Society Workshop on Biometrics*, 2008.
- [8] Marta Gomez-Barrero, Javier Galbally, Julian Fierrez, Javier Ortega-Garcia, and Rejean Plamondon. Enhanced on-line signature verification based on skilled forgery detection using sigma-lognormal features. In *Proc. IEEE/IAPR Int. Conf. on Biometrics, ICB*, pages 501–506, May 2015.
- [9] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba, J. Ortega-Garcia, and D. Maltoni. An on-line signature verification system based on fusion of local and global information. In *Proc. 5th IAPR Intl. Conf. on Audio- and Video-based Biometric Person Authentication, AVBPA*, volume 3546 of *LNCS*, pages 523–532. Springer, July 2005.
- [10] J. Fierrez and J. Ortega-Garcia. Function-based on-line signature verification. *Springer*, pages 225–245, 2008.
- [11] R. Tolosana. Estudio de interoperabilidad en sistemas biométricos de firma manuscrita dinámica. *TFG. Escuela Politécnica Superior, Universidad Autónoma de Madrid*, 2014.
- [12] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia. Benchmarking desktop and mobile handwriting across cots devices: the e-biosign biometric database. *PLoS ONE*, 12(5):1–17, 2017.
- [13] M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally. Mobile signature verification: Feature robustness and performance comparison. *IET Biometrics*, 2014.

- [14] Ruben Tolosana, Ruben Vera-Rodriguez, Javier Ortega-Garcia, and Julian Fierrez. Pre-processing and feature selection for improved sensor interoperability in online biometric signature verification. *IEEE Access*, 3:478 – 489, May 2015.
- [15] E. Gonzalez-Sosa, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia. Reconocimiento biométrico basado en la forma del cuerpo usando imágenes en la banda mmw. In *Proc. Jornadas de Reconocimiento Biométrico de Personas, JRBP*, pages 42–53, September 2013.
- [16] Dit-Yan Yeung, Hong Chang, Yimin Xiong, Susan E. George, Ramanujan S. Kashi, Takashi Matsumoto, and Gerhard Rigoll. Svc2004: First international signature verification competition. In *Proc. ICBA*, volume 3072, pages 16–22, 2004.
- [17] J. Galbally, J. Fierrez, M. R. Freire, and J. Ortega-Garcia. Feature selection based on genetic algorithms for on-line signature verification. In *Proc. IEEE Workshop on Automatic Identification Advanced Technologies, AutoID*, pages 198 – 203, June 2007.
- [18] Anil K. Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 2005.
- [19] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia. Do you need more data? the Deepsigndb on-line handwritten signature biometric database. *ICDAR*, 2019.
- [20] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. Deep-sign: Deep on-line signature verification. *arXiv preprint arXiv:2002.10119*, 2020.
- [21] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. Exploring recurrent neural networks for on-line handwritten signature biometrics. *IEEE Access*, pages 1 – 11, 2018.
- [22] S. Lai and L. Jin. Recurrent adaptation networks for online signature verification. *IEEE Transactions on Information Forensics and Security*, pages 1 – 14, 2018.
- [23] C. Li, F. Lin X. Zhang, Z. Wang, J. Liu, R. Zhang, and H. Wang. A stroke-based rnn for writer-independent online signature verification. In *Proc. International Conference on Document Analysis and Recognition (ICDAR)*, 2019.
- [24] X. Wu, A. Kimura, B. K. Iwana, S. Uchida, and K. Kashino. Deep dynamic time warping: End-to-end local representation learning for online signatura verification. *2019 International Conference on Document Analysis and Recognition (ICDAR)*, September 2019.
- [25] X. Wu, A. Kimura, and K. Kashino. Prewarping siamese network: Learning local representations for online signature verification. *2019 ICASSP - IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2019.
- [26] J. Ortega-Garcia, J. Fierrez-Aguilar, and et al. Mcyt baseline corpus: A bimodal biometric database. *Proc. IEEE Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet*, 150(6):395–401, 2003.
- [27] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. Freire, F. Alonso-Fernandez, D. Ramos, D. Toledano, J. Gonzalez-Rodriguez, J. Siguenza, and J. Garrido-Salas et al. Biosecurid: A multimodal biometric database. *Pattern Analysis and Applications*, 13(2):235–246, 2010.
- [28] J. Ortega-Garcia, J. Fierrez, and et al. The multi-scenario multi- environment biosecure multimodal database (bmdb). *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 32(6):1097–1111, 2010.

- [29] M. A. U. Khan, M. K. K. Niazi, and M. A. Khan. Velocity-image model for online signature verification. *IEEE Trans. on Image Processing*, 15(11):3540–3549, 2006.
- [30] T. Hastie, E. Kishon, M. Clark, and J. Fan. A model for signature verification. In *Proc. IEEE Int. Conf. Systems, Man, Cybernetics*, volume 1, pages 600–604, July 1991.
- [31] A. Sharma and S. Sundaram. On the exploration of information from the dtw cost matrix for online signature verification. *IEEE Transactions on Cybernetics*, 48(2):611–624, February 2018.
- [32] D. Impedovo, G. Pirlo, M. Diaz, and M. A. Ferrer. Wighted direct matching points for user stability model in multiple domains: A proposal for on-line signature verification. *2019 International Conference on Document Analysis and Recognition (ICDAR)*, 2019.
- [33] R. Plamondon and M. Djoua. A multi-level representation paradigm for handwriting stroke generation. *Human Movement Science*, 25(4-5):586–607, September 2006.
- [34] J. Galbally, R. Plamondon, J. Fierrez, and J. Ortega-Garcia. Synthetic on-line signature generation. part i: Methodology and algorithms. *Pattern Recognition*, 45(7):2610–2621, 2012.
- [35] P. Delgado. Generación sintética de secuencias temporales a través de redes neuronales profundas. *TFM. Escuela Politécnica Superior, Universidad Autónoma de Madrid*, 2020.
- [36] Ruben Tolosana, Ruben Vera-Rodriguez, and Julian Fierrez. Biotouchpass: Handwritten passwords for touchscreen biometrics. *IEEE Transactions on Mobile Computing*, 2019.
- [37] Ruben Tolosana, Ruben Vera-Rodriguez, Richard Guest, Julian Fierrez, and Javier Ortega-Garcia. Complexity-based biometric signature verification. In *Proc. 14th IAPR Int. Conference on Document Analysis and Recognition, ICDAR*, November 2017.
- [38] Ruben Vera-Rodriguez, Ruben Tolosana, Javier Hernandez-Ortega, Aythami Morales, Julian Fierrez, and Javier Ortega-Garcia. Modeling the complexity of biomechanical tasks using the lognormality principle: Applications to signature recognition and touch-screen children detection. In *Proc. IAPR Intl. Conf. on Pattern Recognition and Artificial Intelligence, ICPRAI*, May 2018.
- [39] Ruben Vera-Rodriguez, Ruben Tolosana, Miguel Caruana, Gustavo Manzano, Carlos Gonzalez-Garcia, Julian Fierrez, and Javier Ortega-Garcia. Deepsigncx: Signature complexity detection using recurrent neural networks. In *Proc. 15th International Conference on Document Analysis and Recognition, ICDAR*, September 2019.